분야별

차세대인터넷주소 IPv6 실전적용

– 제품제조사 편 –

방송통신위원회
KOREA COMMUNICATIONS COMMISSION
한국인터넷진흥원

CONTENTS

방송통신위원회 KOREA COMMUNICATIONS COMMISSION

한국인터넷진흥원

CHAPTER 04 IPv6 제품 개발 시 고려사항

CHAPTER 05 결언

방송통신위원회 KOREA COMMUNICATIONS COMMISSION
한국인터넷진흥원

그림 목차

표 목차

〈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

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 망사업자, 서비스 제공자, 비즈니스 이용자 등 다른 이해관계자들이 IPv6 인프라를 구축할 수 있어 매우 중요하다.
시장에 IPv6 제품이 다양화 되 있어야 비용 효율적인 IPv6적용이 가능하고 관련 기술의 보편화에도 기여를 하게 된다.

IPv4 신규 할당중지 이후에는 IPv6 주소만 받는 주체들이 점차 늘어갈 것이므로 제품 제조사도 IPv6 지원 장비를 개발하고 수용할 준비가 필요하다. 본 책자는 제품 제조사가 IPv6 제품 개발 시 도움이 될수 있는 관련 정보를 제공하는 것이 목적이다.

2. 대상 및 범위

본 책자는 소프트웨어 및 하드웨어 제조사가 IPv6 제품 제조 시 관련된 기술 표준, IPv6 기반 하드웨어 및 소프트웨어 개발을 위한 프로그래밍 샘플, 관련 인증체계를 기술련 된 표준기술 현황, 시장 현황, 지원 체계 등 여러 고려사항들을 파악할 수 있도록 구성하였다.

제2장

IPv6의 영향을 받는 제품범위

1. 제품범위 분류

IPv6에 영향을 받는 제품들은 네트워크, 서버 및 이용단말, 소프트웨어, 보안 등으로 구분할 수 있다. 아래의 [표 2-1]은 주요 IT 자원의 분류 예시이다. 주로 L3 계층을 다루는 라우터, 운영체제, 방화벽 등은 IPv6 전환에 매우 중요한 요소이며, L2스위치, AP, 단말 자원들도 직간접적으로 IPv6의 영향을 받는다.

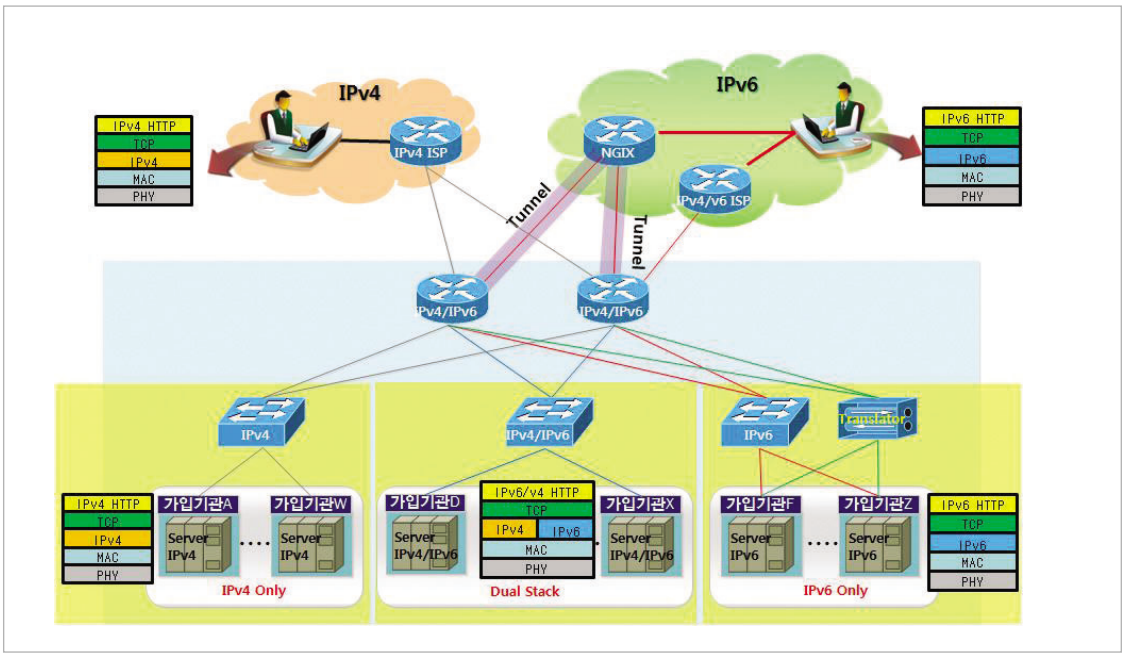
[표 2-1] IPv6의 영향을 받는 제품범위 예

구분	종류
네트워크	• 라우터(edge, border) • 스위치(L2~L7 스위치) • AP(Access point) 장비, NAT 장비
서버 및 이용단말	• 클라이언트(데스크톱PC · 노트북PC 등) • 서버(웹, DB, 인트라넷) • 기타(PDA, 스마트폰, 프린터, 팩스 등) • 음성 · 영상기기(화상회의 등)
소프트웨어	• 운영체제(Windows, Unix, Linux 등) • 데이터베이스(Oracle, Informix, MS-SQL, MySQL 등) • 기타 애플리케이션(DNS, DHCP, FTP, POP, Sendmail, Apache, Tomcat 등)
보안	• 방화벽, IPS, IDS, VPN • 네트워크 접근제어 장치

특히 최근에는 IPTV 등 고품질 서비스가 대중화되면서 L2 스위치에서도 멀티캐스트, DHCP Snoop, Filter 등의 부가 기능들을 사용하고 있는데, 이들 기능들이 IP주소정보를 활용하고 있어 제조사들은 IPv6지원 제품 개발시 L3 이외 부분에 대해서도 면밀히 검토해야 한다.

2. 전환지원 제품

IPv6는 IPv4 환경과 당분간 공존해야 한다. 따라서 아래 그림과 같이 어플리케이션부터 네트워크 계층에 이르기까지 서로 다른 두 개의 프로토콜과 관련된 다양한 연동 시나리오들이 존재한다. 따라서 IPv6로의 전환과정에서 프로토콜 변환(Translation)이나 터널링(Tunneling) 같은 전환 기술을 이용한 제품들이 반드시 필요하다.



다음 [표 2-2]는 IPv4-only 노드, IPv6 노드, 듀얼 스택 노드 등에서 동작하는 클라이언트와 서버 사이의 연결 조합을 요약하였고 'Translator'로 표기된 조합은 노드 사이의 통신이 변환기를 통해서만 연결됨을 나타낸다.

네트워크단의 변환기는 네트워크 노드 간의 상이한 프로토콜을 변환한다. 보통 이용자나 서비스 앞단에 별도 장비로 위치하고, 어플리케이션에 대한 변환을 위해 DNS ALG 등을 탑재한다.

어플리케이션단의 변환기는 보통 OS스택에 적용되어 호스트상의 어플리케이션과 노드 사이에서 변환을 수행한다. 응용프로그램과 링크계층 모듈 간의 전달되는 데이터를 가로채서 IPv4에 관련된 모든 사항을 IPv6로 바꾸어 버리고, 그 반대를 수행하기도 한다. 이 경우 응용프로그램 변경

없이 IPv6 이용이 가능하다. 관련하여 IETF에서 표준화된 기술로는 BIS(Bump-In-the-Stack), BIA(Bump-In-the-API)가 있는데, IETF는 장기적으로 듀얼스택 지원 어플리케이션의 확산을 지향하기 때문에 이들 어플리케이션 변환 솔루션은 불가피한 상황에 사용되는 단기적인 임시 솔루션으로만 권장되고 있다.

변환기술은 현재도 관련 표준이 계속 개선되고 있는데, 어떤 표준을 선택하거나 별도 비표준 기술을 적용하더라도, 장비나 스택자체에서 프로토콜 변환이 정상적으로 완료만 되면 다른 망 구성 요소들에 영향을 미치지 않으므로 벤더의 기술력에 따라 다양한 제품이 나올 수 있는 분야다.

[표 2-2] 클라이언트/서버간의 네트워크 연결 타입

		IPv4 Server Application		IPv6 Server Application	
		IPv4 node	Dual-stack	IPv6 node	Dual-stack
IPv4 Client Application	IPv4 node	IPv4	IPv4	Network Translator	Application Translator
	Dual-stack	IPv4	IPv4	Network Translator	Application Translator
IPv6 Client Application	IPv6 node	Network Translator	Application Translator	IPv6	IPv6
	Dual-stack	Network Translator	Application Translator	IPv6	IPv6

터널링은 IPv4망에 논리적인 터널을 설정해 IPv6 패킷을 전송하는 전환기술로써 터널 엔드포인트 간에 표준기술을 준수해야 한다. 현재 CISCO, Juniper 등 주요 벤더에서 출시되는 대부분의 네트워크 장비는 IETF에서 제정된 표준 터널기술들을 대부분 지원하고 있다.

제3장

IPv6 적용 기술

1. 터널링(Tunneling) 기술

인터넷 트래픽이 IPv6 네트워크에서 인접한 IPv4 네트워크를 통과하여 건너편 IPv6 네트워크로 통신하기 위해 IPv4 네트워크상에 논리적인 터널을 구축하는 기술이다. 대표적으로 설정 터널

[표 3-1] 터널링 구축 기술

방식	종류	사용용도
Configured Tunnels	Router to Router	• Router to Router 동작 • 관리하기에 편리함(6PE)
Automatic Tunnels	6RD(IPv6 Rapid Deployment)	• RFC5969 • 6to4 Tunnel 기반으로 생성 • IPv6 islands를 IPv4망을 통해 연동하는데 사용 • 6RD relay router 에서 자동으로 Encapsulation과 Decapsulation이 가능함 • ISP가 할당 받은 Prefix 사용
	6to4	• RFC 3056 • Router to Router 동작 • IPv6 islands를 IPv4망을 통해 연동하는데 사용 • 2002::/16 prefix 사용 예) 192.0.0.1 2002:c000:0101::/48
	DS-Lite(Dual-Stack Less IPv6 Enabled)	• IPv4 islands를 IPv6망을 통해 연동하는데 사용 • LSN과 연계하여 연동
	Tunnel Brokers	• RFC 3053 • 서버 기반 동작 • www.freenet6.net(Hosted in Canada by Hexago)
	6over4	• RFC 2529 • Host to Router, Router to Router
	IPv4	• IPv4, IPv6 혼재 환경에 적합 • IPv4의 flag 의 “reserved” bit 사용 (DF, MF는 사용하지 않음)
	Teredo	• 사설 IP를 사용하는 서브넷에서 적용 가능
	ISATAP	• 소형 네트워크에 적당

(Configured Tunnel)과 자동 터널(Automatic Tunnel)로 나뉘는데, 사이트간 고정된 터널을 유지할때는 서로 간의 엔드포인트를 상호인식해 터널을 유지하는 Configured Tunnel 기법을 쓰고, 일반 PC 처럼 필요시에만 터널링을 사용하는 경우엔 6to4, 6RD 같은 자동 터널링을 사용한다.

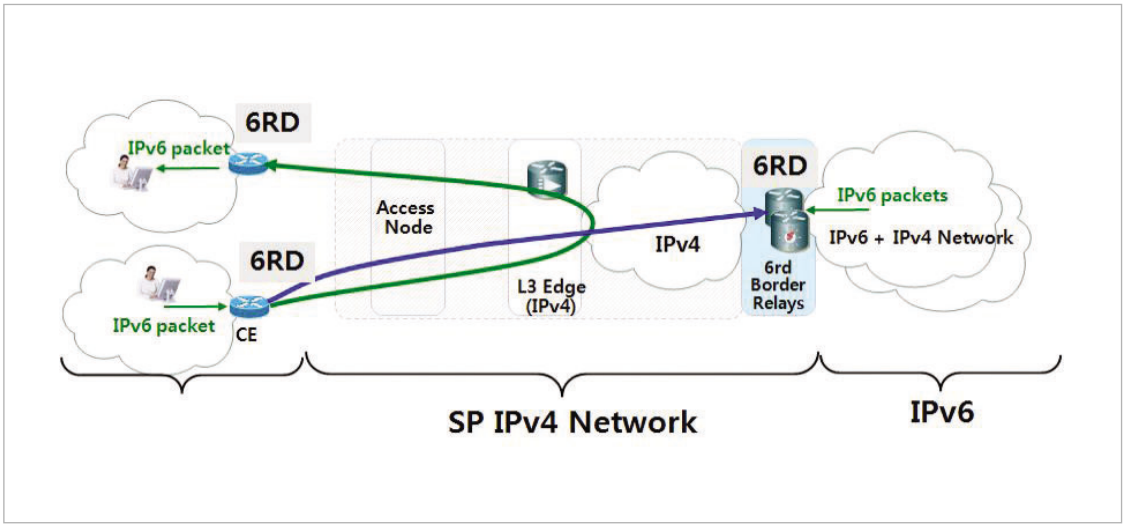
최근에는 전 세계적으로 6to4 tunnel 기반으로 형성된 6RD를 많이 사용하여 연동을 하고 있으며, 일본에서는 DS-Lite Tunnel 기반위에 LSN 변환 기술을 사용하여 FTTH 망에서 서비스를 시행하고 있다.

6RD (IPv6 Rapid Deployment)

6RD는 6to4 Tunnel을 기반에서 나온 기술로써(RFC5969) CPE간 그리고 6RD relay router와의 통신을 가능하게 해주는 Tunneling 기술이다.

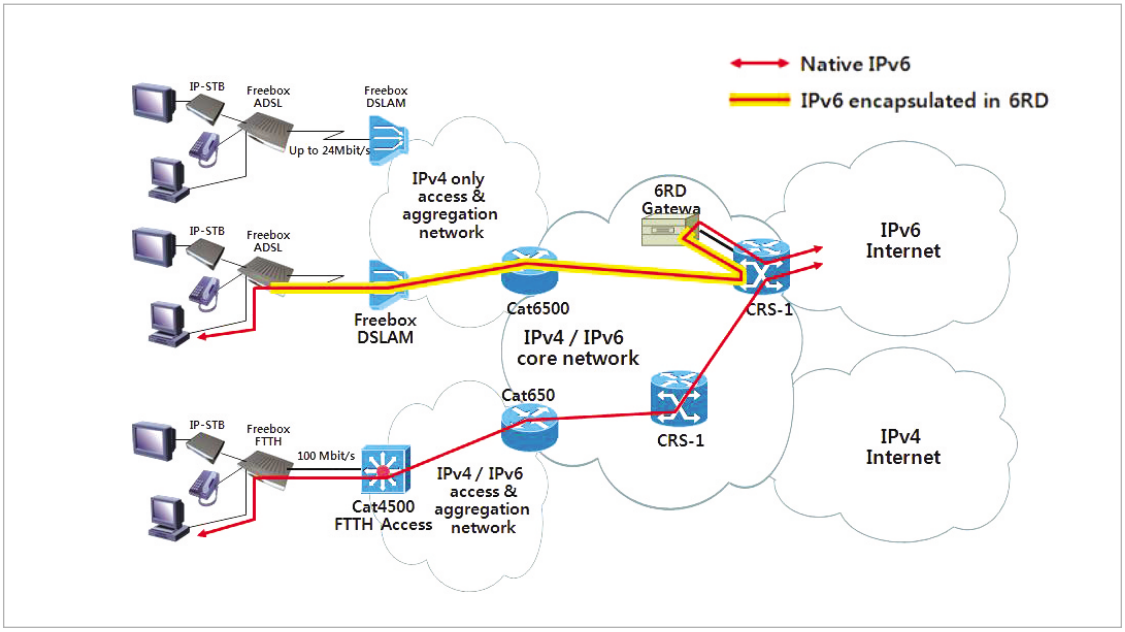
6to4와 다르게 6RD는 고정된 prefix가 아닌 ISP에서 할당받은 prefix를 기반으로 패킷을 형성하며 6RD relay router 와 Tunnel을 형성하여 IPv4망을 통하여 IPv6로 통신을 가능하게 해준다.

[그림 3-1] 6RD 구성



6RD를 사용함으로써 CPE에서 자동설정이 가능하게 되며 Tunnel의 End-point를 쉽게 찾을 수가 있다. 또한 6RD 는 고성능의 Tunnel로서 다른 IPv6 Tunnel보다 많은 가입자를 수용할 수 있어 적은 투자비용과 추가적인 비용을 절감할 수 있다.

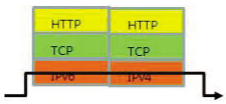
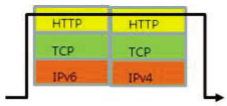
[그림 3-2] Free Telecom 6RD 적용 사례



2. IPv4-IPv6 변환(translation) 기술

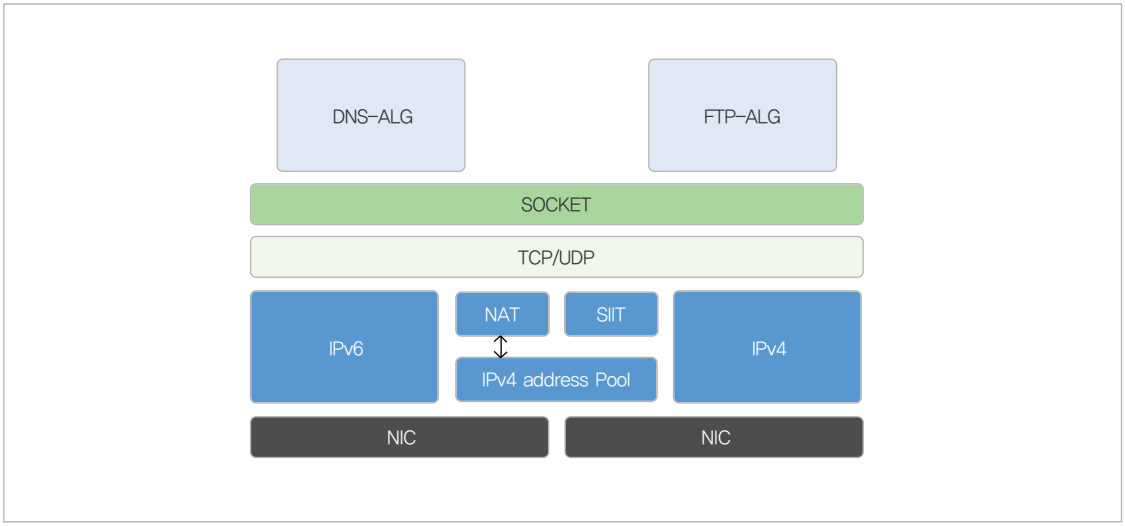
IPv4/IPv6 변환 기술은 IPv4 패킷과 IPv6 패킷을 상호 변환해주는 기술로 듀얼스택 및 터널 적용이 어려운 경우 사용된다. 변환방식에 따라 장단점이 있으므로 기술적 특징을 이해하고 운영 중인 망에 적합한 변환방식을 채택해야 한다.

[표 3-2] 변환 기술

변환 방식		특징
Header Conversion		• 장점 : IP/ICMP 헤더만 변환해 빠름 • 단점 : 패킷 단편화(fragmentation) ICMPv4와 ICMPv6 간의 상이함에 따른 문제
Transport Relay		• 장점: 서비스에 독립적, TCP/UDP Relay 가능 • 단점 : Header conversion보다 느림
Application Proxy		• 장점 : 주소 매핑 불필요 • 단점 : 각 서비스별로 독립된 서버를 사용해야하고 느림

NAT-PT (Network Address Translation - Protocol Translation, RFC2766)는 헤더 변환 기법인 SIIT[1]를 기반으로 어플리케이션별 ALG를 통해 IPv4↔IPv6 간의 변환을 제공한다.

[그림 3-3] NAT-PT(RFC2766) 기본 구조



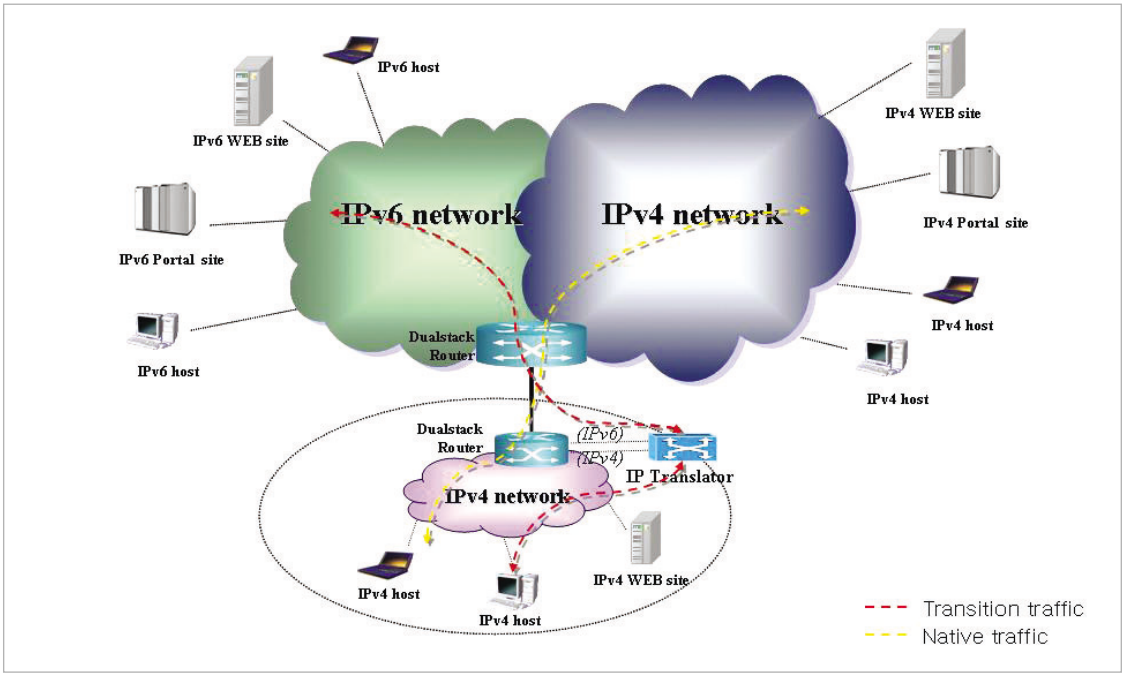
동적으로 주소를 할당하고 변환하기 위해서는 응용서비스에 따라 추가적인 요구사항이 발생하는데, 이를 지원하기 위한 ALG(Application Level Gateway)를 사용한다. 하지만 ALG는 새로운 응용이 나올 때 마다 추가해야 하는 문제가 있고 단대단(End-to-End) 연결을 저해하는 또 하나의 NAT의 확산으로 인식되어 기존의 NAT-PT 표준은 표준제정 기구인 IETF에서 일단 폐기된 상태이다.[2] 또한 기존 표준으로는 망 사업자 수준의 트래픽 변환에는 무리가 있어 현재 IETF에서 이를 개선하여 새로운 기술을 표준화하기 위한 논의가 진행중이다.

표준은 폐기되더라도 이미 구축된 기존 NAT-PT 장비를 사용하는 데는 문제가 없다. 프로토콜만 변환이 된다면 향후 나오는 표준들과는 독립적으로 운영될 수 있다. 예를 들어 기업내의 VoIP 서비스, 프린터 네트워크, 기타 Legacy 망 등 당장 외부망과 연동이 필요 없고 신규장비 대개체시 자연스럽게 IPv6로 전환하는 서비스의 경우 목적에 맞는 ALG에 한정해서 NAT-PT를 활용할 수 있다.

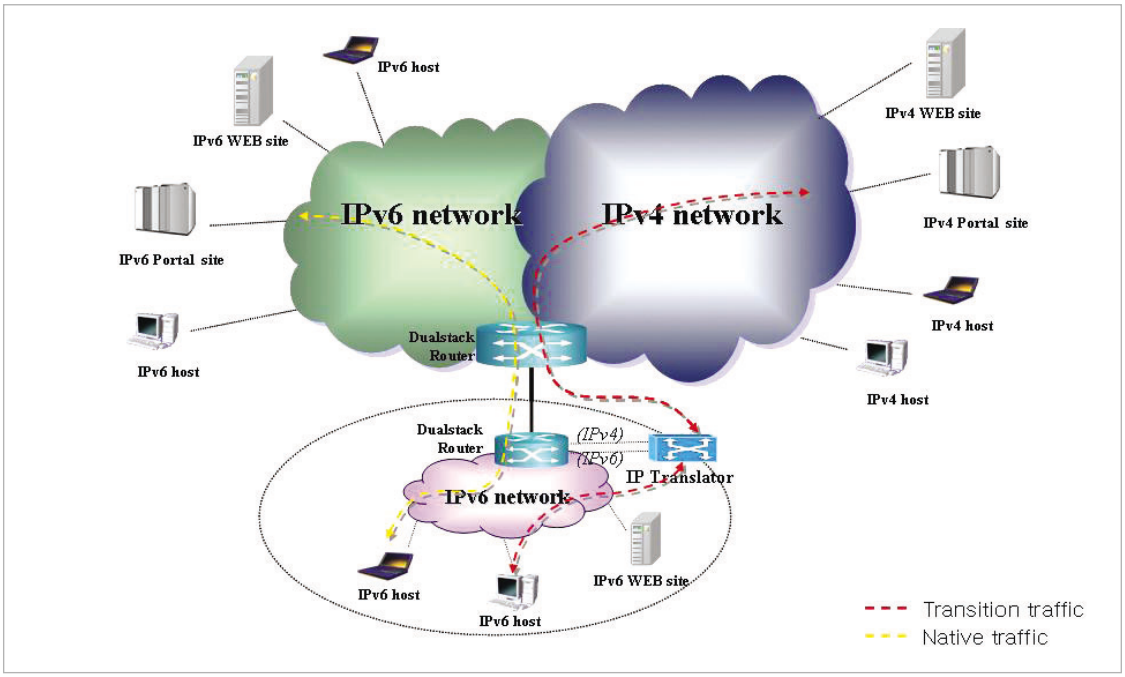
[그림 3-4], [그림 3-5]는 변환장비를 이용한 IPv4 ↔ IPv6 망간 구성 예이다.

1) Stateless IP/ICMP Translator
2) RFC4966, Reasons to Move the Network Address Translator - Protocol Translator(NAT-PT) to Historic Status

[그림 3-4] 변환장비를 이용한 IPv4 → IPv6 구성 예

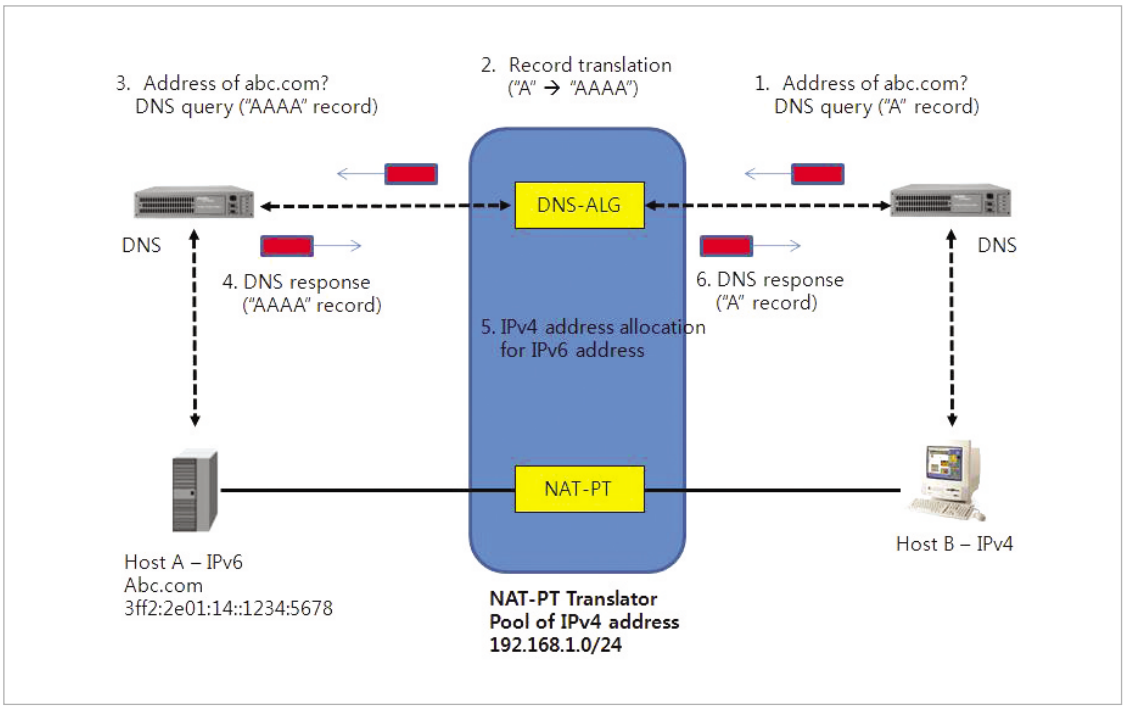


[그림 3-5] 변환장비를 이용한 IPv6 → IPv4 구성 예



변환장비 설치 시 IPv4 패킷의 착신지 주소에 대한 라우터는 변환장비의 변환 주소로 설정한 IPv4 주소 Pool에 대한 라우팅 경로를 변환장비의 IPv4 포트의 인터페이스 주소를 설정하고, 변환장비는 DNS Proxy 기능과 정적 또는 동적인 IPv4/IPv6 주소 맵핑에 따라 IPv4/IPv6 변환을 수행한다. IPv4 가입자는 자신이 보내는 패킷이 IPv4 망으로 가는지 아니면 IPv6 망으로 가는지 의식할 수 없으며, 착신지 주소가 라우터에 의해 변환장비로 라우팅 되는 패킷은 IPv6 패킷으로 변환되어 라우터로 전송되고, IPv6 라우팅에 의하여 IPv6 망으로 보내지게 된다.

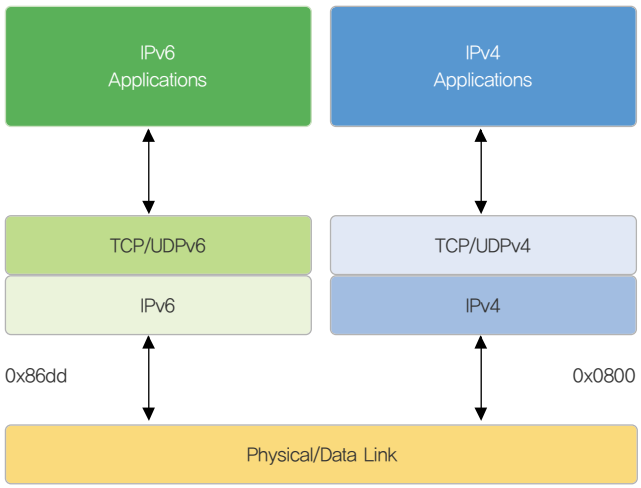
[그림 3-6] 변환장비 동작 방식



기존의 IPv4 가입자의 IPv4 망 접근은 Dualstack 라우터를 통해 기존과 동일하게 이루어진다. 이때 라우터가 단일 스택장비이면 IPv4 라우터와 IPv6 라우터가 각각 변환장비와 연동될 것이며, 듀얼스택이 지원되는 장비라면 1대의 라우터가 IP 변환기와 연동될 것이다.

3. IPv4/IPv6 듀얼스택

[그림 3-7] 듀얼스택 구조



듀얼스택은 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 네트워크상의 노드는 IPv4 노드와 통신하기 위해서는 IPv4 스택을 사용하고, IPv6 노드와 통신을 하기 위해서는 IPv6 스택을 사용한다.

제4장

IPv6 제품 개발 시 고려사항

1. 관련 기술 표준화 현황

IPv6 기술 표준화는 IETF의 IPv6와 v6ops 워킹그룹 등을 중심으로 관련 그룹들과 협력하여 진행되고 있다. IPv6 기술을 개념적으로 분류해 보면 망 계층 프로토콜 및 주소체계를 다루는 기본 기술 IPv6에 특화된 응용 기술 IPv4 망에서 IPv6로의 전환 및 타 망과의 연동을 다루는 IPv6 변환연동 기술과 IPv6 상용 망과 실험 망 구축을 포함한 망 구축 기술 등이 있다.

1.1 국내외 관련 표준화 문서 리스트

현재 IETF에서 IPv6와 관련된 표준화 작업이 진행 중에 있다. IPv6와 관련된 여러 워킹그룹들이 표준화 작업을 진행하고 있으며 아래는 각각의 워킹그룹에서 담당하고 있는 IPv6 표준화 내역이다.

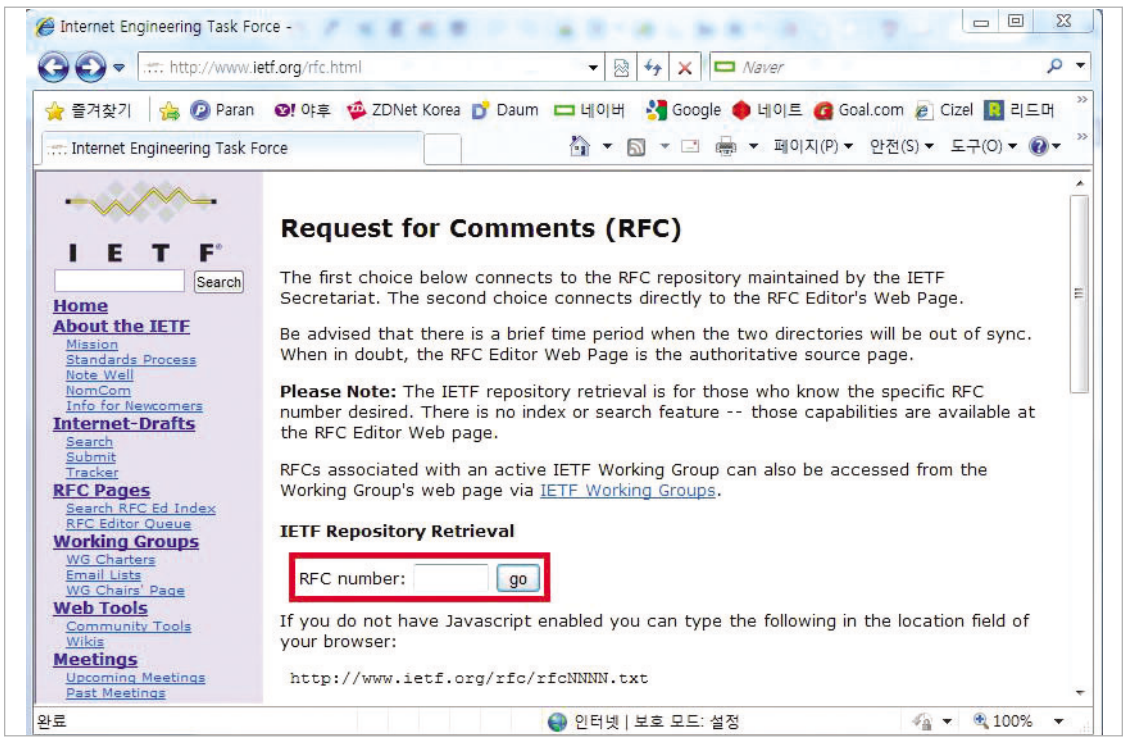
[표 4-1] IETF IPv6 관련 Working Group

Area	Working Group	표준화
Internet	6lowpan	IPv6 over Low power WPAN
	6man	IPv6 Maintenance
	autoconf	Ad-Hoc Network Autoconfiguration
	dhc	Dynamic Host Configuration
	dnsext	DNS Extensions
	mipshop	Mobility fot IP: Signaling and handoff Optimization
	mext	Mobility EXTensions for IPv6
	netlmm	Network-based Localized Mobility Management
	ntp	Network Time Protocol
	softwire	Softwires
	shim6	Site Multihoming by IPv6 Intermediation

Op & Mgmt	v6ops	IPv6 Operations
	dime	Diameter Mainrenance and Extensions
	dnsop	Domain Name System Operations
	radext	RADIUS EXTensions
Routing	bfd	Bidirectional Forwarding Detection
	idr	Inter-Domain Routing
	isis	IS-IS for IP Internets
	l3vpn	Layer 3 Virtual Private Networks
	ospf	Open Shortest Path First IGP
	vrrp	Virtual Router Redundancy Protocol

각각의 워킹그룹에서 진행된 표준화 작업이 완료된 RFC 문서는 부록에서 확인 가능하다. 표준화 된 IPv6 RFC 문서는 코어 프로토콜, 보안, 무선 환경에서의 이동성 등과 같은 여러 분류로 나눠진다. 워킹그룹에서 표준화 작업이 완료된 IPv6 RFC 문서에 대해서는 홈페이지에서 확인할 수 있다.

[그림 4-1] RFC 문서 검색 및 확인

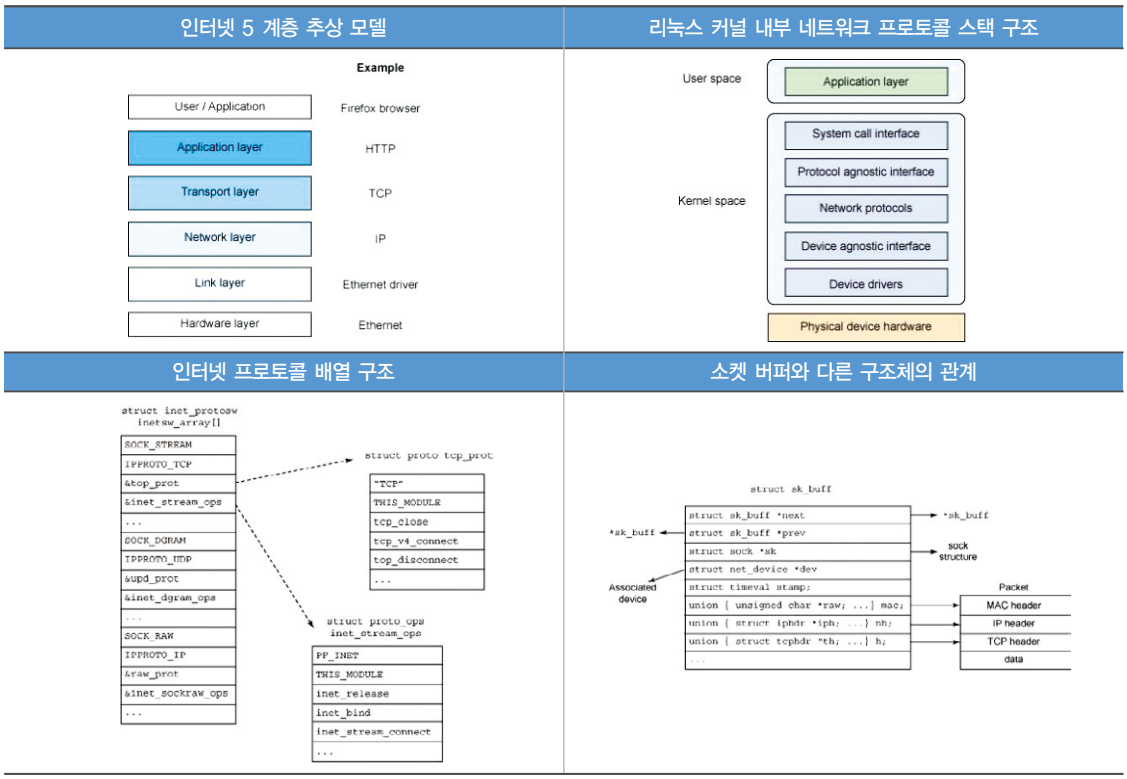


2. IPv6기반 통신 장비의 개발

IPv6 서비스(응용S/W)를 개발하기 이전에, IPv6망 기반환경 구축이 필수적이며, IPv6기반 네트워크 · 통신 장비(라우터, 스위치등)의 도입이 필수적이다. 하드웨어 설계등 전자공학적인 지식을 생략하고 시스템S/W개발 관점에서 장비 개발절차를 간략히 설명하면 다음과 같다.

IPv6기반 장비를 개발하기 위해서는 운영체제 내부 네트워크 프로토콜 스택 소스코드를 이해하고 장비 개발 시 적용해야 한다. 기존 소스코드의 단순 적용 수준이 아니라, 표준(RFC 2460)에 의거해 정확하게 작성되어야 한다. 시스템 안정성을 위해 본 문서 4절에서 소개될 IPv6 인증이 필요하다. IPv6 인증체계의 경우 IPv6 기반 네트워크 · 통신 장비가 표준적합성에 맞게 정확하게 구현되었는지 검증하기 위한 프로그램이며, 각 장비 제조사들은 이에 대한 준비가 필요하다.

[그림 4-2] IPv6 장비 개발을 위한 네트워크 프로토콜 스택 구현원리

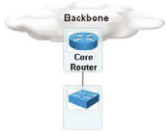


새로운 개발 장비를 위해 운영체제 커널 내부의 네트워크 프로토콜 스택을 분석하는 것은 무척 난해하고, 많은 시간이 소요된다. 작업 간에 리눅스, Free BSD 등 오픈소스기반 운영체제 소스코

드를 참고하면 수월하게 진행될 수 있다. 그러나 앞서 설명한 대로 다른 벤더 장비들과의 정확한 통신을 위해서 표준에 맞게 구현되었는지 여부를 점검해야 해야 한다. 장비개발자는 RFC 2460을 기준으로 각자의 전문영역의 IPv6 관련 표준문서를 통해 프로토콜을 먼저 이해하고, C언어와 리눅스커널(네트워크 스택영역)에 대한 학습이 필요하다.

제품 제조사는 IPv6 장비 개발시 아래와 같은 기능들을 고려해야 한다.

[표 4-2] 주요 네트워크 제품별 IPv6 고려사항

구분	구성장비	종류	IPv6 기능	비고
백본망		라우터/스위치	• IPv6 주소 입력 가능 • IPv6 라우팅 기능 • SNMP 등 관리 기능 • 보안관련 기능 • NTP 기능 • DHCPv6 기능	
서비스망		방화벽	• IPv6 주소 입력 가능 • IPv6 라우팅 기능 • SNMP 등 관리 기능 • 보안관련 기능(Filtering)	
		L4	• IPv6 주소 입력가능 • IPv6 라우팅 기능 • SNMP 등 관리기능 • 보안관련 기능 • 로드밸런싱 기능	
		NMS	• IPv6 주소 입력 기능 • IPv6 모니터링 관리기능 • SNMPv6 MIB 처리기능 • WEB BASE GUI 기능 • SSH등 보안기능	
		VOD	• IPv6 주소 입력 기능 • DNP For VoD 기능 • SSH 등 보안 기능 • Streaming For VoD 기능 • NMS 등 관리기능	

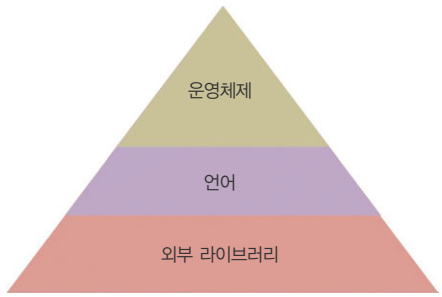
3. IPv6기반 응용S/W 개발을 위한 프로그래밍 언어별 API현황

본 문서는 IPv6 장비를 생산하는 장비 밴더들을 대상으로 주로 작성하였으나, IPv6 제품들 중, 응용계층에서 동작하는 제품들이 존재하므로(예: 터널브로커, Socks based Gateway, ALG모

듈, 보안장비 등) 개발환경에 고려가 필요하다. 또한, 통신망 전환 뿐만 아니라, IPv6기반 응용 S/W개발도 병행해서 진행해야 하므로 IPv6 전환 시 응용S/W 개발자들을 위한 프로그래밍 언어별 IPv6기반 통신API제공에 대해 간략히 설명한다.

프로그래밍 언어에서 IPv6 API(외부라이브러리, 객체지향언어의 경우 클래스라고도 함)를 지원하는지 확인 하여야 한다. 각 프로그래밍 언어별 IPv6를 대응할 수 있는 API는 다음과 같다.

〈IPv6 대응하기 위한 3가지〉



[표 4-3] 프로그래밍 언어별 IPv6통신 API

	IPv6 지원	라이브러리	지원 사이트
C/C++	O	AF_INET6	http://msdn.microsoft.com/
.NET	O	AddressFamily.InterNetworkv6	
JAVA	O	java.net.Inet6Address	http://java.sun.com/
Perl	O	IO::Socket::INET6	http://www.perl.org/

3.1 C/C++ 구현의 예

[표 4-4] C/C++ 샘플 코드

```
struct sockaddr_in6 sin6;
socklen_t salen;
struct hostent *hp;

s = socket(AF_INET6, SOCK_STREAM, IPPROTO_TCP);

/* DNS name lookup - does not support scope ID */
hp = gethostbyname2(hostname, AF_INET6);

memset(&sin6, 0, sizeof(sin6));
sin6.sin6_family = AF_INET6;
salen = sin6.sin6_len = sizeof(struct sockaddr_in6);
memcpy(&sin6.sin6_addr, hp->h_addr, sizeof(sin6.sin6_addr));
sin6.sin6_port = htons(80);
if (connect(s, (struct sockaddr *)&sin6, salen) 0) {
perror(""connect"");
exit(1);
}
```

3.2 .NET 구현의 예

[표 4-5] .NET 샘플 코드

```
const int PORT=2001;
Socket listener = new Socket(
    AddressFamily.InterNetworkV6,
    SocketType.Stream,
    ProtocolType.Tcp);
listener.Bind(new IPEndPoint(IPAddress.IPv6Any, PORT));
listener.Listen(0);
```

(출처: http://www.codeproject.com/KB/IP/ipv6.aspx)

3.3 JAVA 구현의 예

[표 4-6] JAVA 샘플 코드

```
int ServSock, csock;
struct sockaddr addr, from;
...
ServSock = socket(AF_INET6, SOCK_STREAM, PF_INET6);
bind(ServSock, &addr, sizeof(addr));
do {
        csock = accept(ServSocket, &from,
        sizeof(from));
        doClientStuff(csock);
} while (!finished);
```

3.4 Perl 구현의 예

[표 4-7] Perl 샘플 코드

```
use IO::Socket::INET6;
...
$sock = IO::Socket::INET6->new(PeerAddr => 'www.perl.org',
PeerPort => 'http(80)',
Domain => AF_INET ,
Proto    => 'tcp');

$sock = IO::Socket::INET6->new(PeerAddr => 'localhost:smtp(25)');

$sock = IO::Socket::INET6->new(Listen     => 5,
LocalAddr => 'localhost',
LocalPort => 9000,
Proto     => 'tcp');

$sock = IO::Socket::INET6->new('[::1]:25');

$sock = IO::Socket::INET6->new(PeerPort  => 9999,
PeerAddr  => Socket6::inet_ntop(AF_INET6,in6addr_broadcast),
Proto     => udp,
LocalAddr => 'localhost',
Broadcast => 1 )
or die "Can't bind : $@\n";
```

3.5 IPv6기반 주요 응용소프트웨어의 예

서버장비의 경우, 사용 중인 운영체제상에 IPv6 스택이 구현되어 있는지 여부를 확인해봐야 한다. 범용 DNS, E-mail 소프트웨어의 경우 IPv6기능이 지원되는 경우가 많다. 그러나, 전자결제, 업무관리시스템등 레거시 S/W상에 IPv6기능을 업데이트할 경우, 일정 예산이 발생하고 소스코드레벨에서 다시 유지보수가 필요할 수도 있다. 서버장비에서 주로 사용되는 IPv6기반 범용 응용소프트웨어의 예는 다음과 같다.

[표 4-8] IPv6지원 서버용 운영체제 및 응용 S/W

서버장비를 위한 IPv6지원 운영체제 최저버전		
'Windows Server 2000', 'OpenBSD 2.7', 'Linux Kernel 2.2', 'Solaris 5.8', 'HP-UX 11i', 'FreeBSD 4',		
IPv6기반 범용 응용소프트웨어		
서비스 종류	소프트웨어 명	버전
DNS	BIND 9	BIND 8.4.6이상(현재 BIND 9)
	Microsoft DNS	Windows 2003이상(현재 2008)
이메일	Sendmail	8.8.0이상(현재 8.14.3)
	exim	1.9x이상(현재 4.69)
	zmailer	1.99.26이상(현재 2.99.57)
	postfix	2.2.0이상(현재 2.5.5)
웹서비스	Apache	2.0이상(현재 2.2.9)
	Tomcat	4.0이상(현재 6.0.18)
	WebtoB	4.1이상
	JRun	4.0이상

4. 관련 인증체계 현황(IPv6 Ready Logo, CC인증 등)

4.1 IPv6 Ready Logo Program

[그림 4-3] IPv6 Ready Logo 홈페이지 화면

국제 IPv6 Forum이 IPv6 프로토콜을 탑재하고 있는 네트워크 장비의 신뢰성 확보 및 기술보급을 위해 2003년 9월부터 시행중인 인증제도이며, 이를 추진하기 위한 추진체로 IPv6 Forum은 v6 Logo Committee(v6LC)를 구성하여 운영하고 있다. IPv6 Ready Logo 프로그램은 정해진 시험규격에 의해 검증된 제품에 대해 IPv6 Ready Logo를 발급하는 제도를 말하며, 세부 시험규격에 따라 Phase I, Phase II 그리고 Phase III(예정) 인증으로 구분되어 실시되고 있다.

4.1.1 시험 범위 및 인증 기준

Ready Logo의 Phase I 시험규격은 IPv6 Router와 Host로 대분류하여 작성되어 있으며 분류기준은 RFC 2460에 명시된 바에 의해 구분된다. Phase II 시험규격은 Phase-I의 내용을 포함하고, 보안, 무선 환경에서의 이동성과 같은 다양한 확장 규격을 요구한다. 또한 각 시험규격은 공통된 시험 범위를 가지고 있으며 관련 표준이 정하는 역할에 의거하여 적합성 시험 및 상호 운용성 시험을 수행한다.

적합성 시험이란 표준에 명시된 특정기능에 대해 장비의 올바른 구현여부를 시험하는 것으로 IPv6 Ready 위원회는 Host와 Router와 관련하여 각각 200여개의 시험항목을 준비해 놓고 있다. 시험통과를 위한 기준은 모든 시험항목에 100% 통과를 하여야 한다. 이를 시험하기 위한 시험용 소프트웨어는 Self Testing Tool이라 하며, IPv6 Ready Logo 홈페이지에서 구할 수 있다.

상호 운용성 시험은 시험규격에서 정하는 해당 기능에 대해 서로 다른 장비가 표준에 따라 상호연동 가능한지를 판단하는 시험으로, 자신의 장비가 무엇이든지 관계없이, 상호연동이 가능한 장비를 최소한 4개 이상 확보하여야 한다. 또한 장비의 종류에 따라 2종 이상의 라우터 및 2종 이상의 호스트를 필수적으로 포함하여야 한다. 현재까지 고려하고 있는 각 단계별 세부 관련 표준은 다음과 같다.

[표 4-9] Phase I & II 시험 규격

Phase I	IPv6 Core Protocols (Host, Router, Special Devices)
Phase II	IPv6 Core Protocols (Host, Router)
	IPsec (End-Node, Security Gateway)
	IKEv2 (End-Node, Security Gateway)
	MIPv6 (Correspondent Node, Home Agent, Mobile Node)
	NEMO (Home Agent, Mobile Router)
	DHCPv6 (Client, Server, Relay Agent)
	SIP (UA, Endpoint, B2BUA, Proxy, Register)
	Management (SNMP-MIBs) (Agent, Manager)

Ready Logo의 Phase II는 다양한 시험 규격을 요구하기 때문에 자세한 Phase II 시험 규격은 아래의 주소 및 부록에서 확인할 수 있다.

Phase II : https://ipv6ready.org/?page=phase-2-tech-info

4.1.2 국내외 IPv6 Ready Logo 인증 IPv6 제품 리스트

2010년 7월 기준으로 432개의 제품이 Phase I(Silver) IPv6 Ready Logo를 획득했으며 365개의 제품이 Phase II(Gold) IPv6 Ready Logo를 획득하였다. Phase I은 은색로고(Silver Logo)를 사용하며 IPv6 Core Protocol에 대한 기본적인 인증만 수행한다. Phase II는 금색로고(Gold Logo)를 사용하며 Phase I의 내용을 포함하고 다양한 확장 규격을 요구한다. 다음은 일부 IPv6 Ready Logo를 획득한 제품이다.

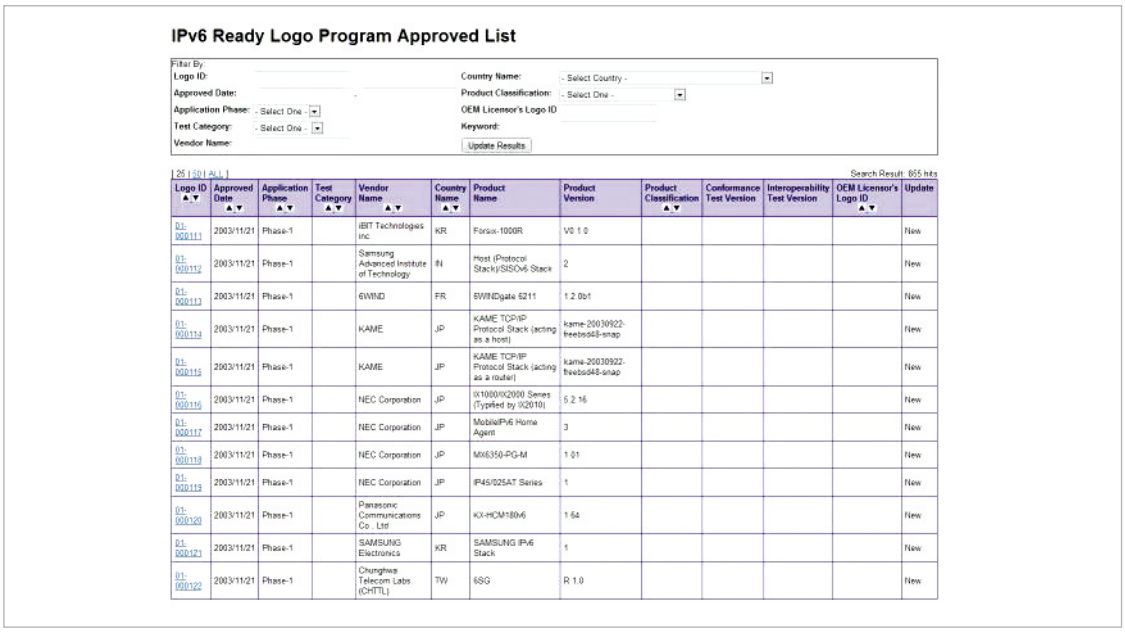
[표 4-10] IPv6 Ready Logo 획득한 제품

획득 날짜	회사	제품
20031121	iBIT Technologies inc	Forsix-1000R
20031121	SAMSUNG Electronics	SAMSUNG IPv6 Stack
20040326	Cisco Systems	Cisco 12000 series
20040326	Microsoft Corporation	Windows
20040914	IBM	AIX 5L
20060926	SUN Microsystems Inc	Solaris
20100623	Radware LTD	AppDirector
20100713	OULLIM Information Technology	SECUREWORKS 200

IPv6 Ready Logo를 획득한 국내외 제품 리스트는 아래 주소에서 확인할 수 있다.

https://www.ipv6ready.org/db/index.php/public/

[그림 4-4] IPv6 Ready Logo 획득 제품



4.1.3 IPv6 Ready Logo 인증 절차

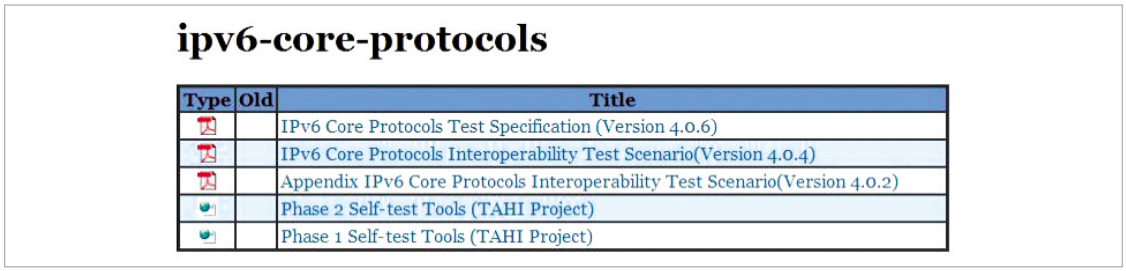
IPv6 Ready Logo Phase I 과 Phase II의 인증 절차는 똑같다. 테스트에 사용되는 제품들은

시험 규격에 대해 100% 통과를 해야 한다.

① IPv6 Ready Logo 홈페이지에서 IPv6 Ready Logo Test Specification을 다운로드 한다.

② Phase I & Phase II Self-test Tools를 다운로드 하거나 IPv6 Interoperability Test Scenario를 다운 받아서 IPv6 Ready Logo를 획득하려는 제품으로 테스트를 진행하면 된다. 테스트하려는 제품을 IPv6 Ready Logo Approved Test Laboratory에 제출하여 테스트를 진행해도 가능하다. Approved Test Laboratory에는 TTA(Korea), BII(China), CHT-TL(Taiwan), IRISA(France), 그리고 UNH-IOL(US) 등이 있다.

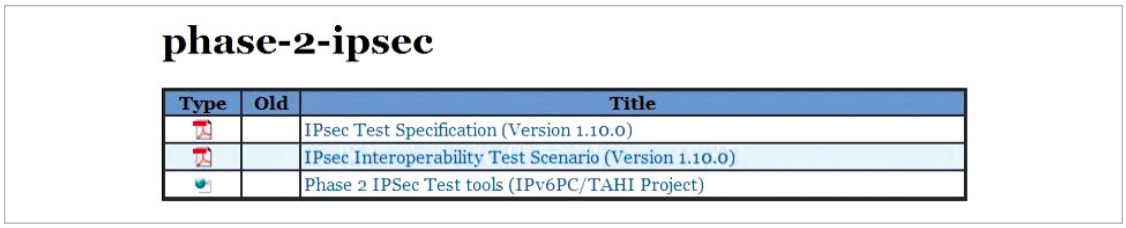
[그림 4-5] Phase I Test Specification



ipv6-core-protocols

Type	Old	Title
		IPv6 Core Protocols Test Specification (Version 4.0.6)
		IPv6 Core Protocols Interoperability Test Scenario(Version 4.0.4)
		Appendix IPv6 Core Protocols Interoperability Test Scenario(Version 4.0.2)
		Phase 2 Self-test Tools (TAHI Project)
		Phase 1 Self-test Tools (TAHI Project)

[그림 4-6] Phase II IPsec Test Specification



phase-2-ipsec

Type	Old	Title
		IPsec Test Specification (Version 1.10.0)
		IPsec Interoperability Test Scenario (Version 1.10.0)
		Phase 2 IPSec Test tools (IPv6PC/TAHI Project)

③ 테스트해서 나온 결과 값을 수집한다. (Self-testing Tools와 IPv6 Interoperability Test를 통해서 나온 결과 값 or IPv6 Ready Testing laboratory를 통해 나온 결과 값)

④ IPv6 Ready Logo 홈페이지에서 Application Form을 채워 넣는다.

[그림 4-7] Phase II IPsec Test Specification

```
IPv6 Ready Logo Program Phase-1, Phase-2 IPv6 Core Protocols
Application Form (Available from 2009/06/18)

Application Phase (Phase-1 or Phase-2): _________________

Target Informations:
  Vendor Name:      ___________________________________
  Country Name:     _________________
  Product Name:     ___________________________________
  Product Version:  _________________
  Product Classification (host, router or special device): _________________
  * "Special device" is only for Phase-1.
  Product Description: ____________________________________________

Contact Person:
  Full Name: ___________________________________
  E-mail:    ___________________________________

Test Result:
  * Test evidence should be attached with this application form.

  Version of the Self Test and Interoperability Test
    Test Specification:             _________________
    Self Test Tool:                 _________________
    Interoperability Test Scneario: _________________

  (If Target is OS/Protocol Stack,
   running environment have to be described below.)

  Environment for OS/Protocol Stack: ___________________________________
```

⑤ 작성한 Application Form과 테스트 결과 (Configuration, Command result, Test result, Packet dump file etc)를 첨부하여 v6-appli@ipv6ready.org로 이메일을 보낸다.

[표 4-11] 시험 결과물 및 작성방법

	최종 시험 결과물	결과물 세부사항
적합성 시험	Self-Testing Tool 시행 결과	시험을 수행했던 CT 폴더 내부에 있는 모든 파일을 압축하여 제출
상호운용성 시험 가입자수 (비중, %)	각 노드 기본 정보	각 노드별 기본 정보(OS 명칭 및 버전, 시험에 사용한 주소정보)
	시험망 구성도	시험규격에 정의된 시험망을 활용하여, 각종 주소정보를 기입
	실행명령 결과	Ping Test에 의한 시험 결과물
	TCPdump File	시험 노드와는 상이한 dump node를 활용하여 TCPdump를 수행하여 시험 항목별 결과로 생성
	Test Result Table	시험규격에 의해 정의되어 있는 최종 시험 결과 표에 합격여부 기록

⑥ Usage Agreement Confirmation 페이지 URL과 Application ID를 받게 될 것이고 IPv6 Ready Logo Technical Group의 Examiner가 제조사가 지원한 시험 프로세스에 대해 연락을 할 것이다.

⑦ IPv6 Ready Logo Examiner에 의해 테스트가 시작될 것이다. 만약 연락을 못 받았을 경우

(Phase I은 1달, Phase II는 2주) 다시 v6-appli@ipv6ready.org로 영문으로 이메일을 보낸다.

⑧ IPv6 Ready Logo Technical Group을 통해서 리뷰과정을 진행한 후 만약 테스트에 사용한 제품이 시험 규격에 대해 100% 통과를 하면 IPv6 Forum Logo Regional Officers를 통해 Logo ID와 IPv6 Ready Logo를 사용할 수 있는 권한을 얻게 된다.

⑨ 승인된 제품에 대해서는 Approval Web에 등록이 된다.

⑩ 제품의 업데이트(i.e. version no.)가 있을 경우 v6-appli@ipv6ready.org로 해당 정보를 보내게 되면 확인 후 정보가 수정된다. 해당 이메일에는 Vendor name, Product name, 업데이트 된 제품의 정보, 그리고 Logo ID가 포함이 돼 있어야 한다.

만약 지정된 기관에서 테스트를 진행할 경우 국내의 경우는 TTA에서 시험을 진행할 수 있다. TTA 홈페이지에서는 다양한 시험인증 서비스를 제공하고 있다. 지원 양식을 다운받아서 신청을 할 수 있고 온라인으로 IPv6 Ready Logo 테스트를 신청할 수 있다.

[그림 4-8] IPv6 Ready Logo 시험 절차 및 신청

시험 기간 및 시험 수수료 같은 경우 내 업체들에게는 적정한 할인율을 적용하고 있으므로, 해외 시험장을 활용하는 것보다 많이 저렴하다. 시험 비용은 크게 장비 사용료 및 인건비 부분으로 구성되며, 두 가지 항목은 시험 기간과 밀접한 관련을 맺고 있다. 즉, 시험 비용은 해당 장비를 얼마나 다양한 요소들에 대해 얼마나 오랫동안 테스트 하느냐에 따라 결정된다. 그러므로 일률적인 시험 비용을 산정할 수 없으며 각 항목별 기준비용을 산정해 놓고 투입되는 Resource를 고려하여 시험 비용을 책정한다.

TTA에서 진행되는 IPv6 Ready Logo 시험 같은 경우 1주일정도 소요되나 시험 받고자하는 장비와 시험 종류에 따라 시험기간이 많이 달라지므로, 사전 협의가 필요하다. IPv6 Ready Logo 시험을 받을 경우 해당 장비의 결과치만 제공을 하고 보고서는 제공하지 않는다.

[그림 4-9] IPv6 Ready Logo (Phase I & II)

4.2 TTA IPv6 시험인증

한국정보통신기술협회(TTA)에서는 네트워크 장비, 디지털방송 장비, S/W 및 이동통신 장비에 대해서 시험인증 서비스를 제공하고 있으며 시험 대상 장비 및 기술에 대한 내용은 홈페이지에서 확인할 수 있다. 국내 IPv6 제품에 대하여 TTA가 자체적으로 정한 기준에 따라 시험 후 인증 기준을 만족하는 경우에 TTA Verified 인증서와 인증마크를 부여한다. IPv6 관련 프로토콜에 대한 적합성시험/성능평가 시험서비스를 제공하고 있다.

[그림 4-10] TTA 시험인증연구소 홈페이지 화면

4.2.1 주요 시험 범위

① 적합성 시험

- ✓ IPv6 Core Protocol
- ✓ Transition Mechanisms (NAT-PT/SIIT, 6to4, Configured & Automatic Tunnel)
- ✓ Routing Protocols (RIPng, OSPFv3, BGP4+)
- ✓ Mobile IPv6 (Home Agent, Mobile Node, Correspondent Node)

② 성능 시험

- ✓ L3 forwarding performance
- ✓ Convergence time
- ✓ Route Flapping
- ✓ Route learning

4.2.2 TTA 인증 IPv6 제품 리스트

2010년 7월을 기준으로 네트워크 분야에서 102개의 제품이 TTA Verified 인증을 획득했다. 다음은 일부 TTA Verified 인증을 획득한 제품이다.

[표 4-12] IPv6 TTA Verified 인증 획득 제품

획득 날짜	회사	제품
2004.03.25	㈜아이비트	IPv6 Core Host Stack
2007.02.13	LG-Nortel㈜	IP Phone
2007.10.01	㈜넥스지	VPN/IPv6 Router
2008.09.29	삼성전자㈜	IPv6 Router
2009.04.16	시스코시스템즈코리아㈜	IP PBX
2010.03.03	㈜다산네트웍스	L3 스위치 (v6424)
2010.06.16	㈜안철수연구소	TrusGuard 1000P
2010.06.29	㈜퓨쳐시스템	WeGuardia™ XTM

TTA Verified 인증을 획득한 국내외 제품 리스트는 아래 주소에서 확인할 수 있다.

http://test.tta.or.kr/research/result/

[그림 4-11] TTA Verified 인증 획득 제품

4.2.3 TTA 인증 절차

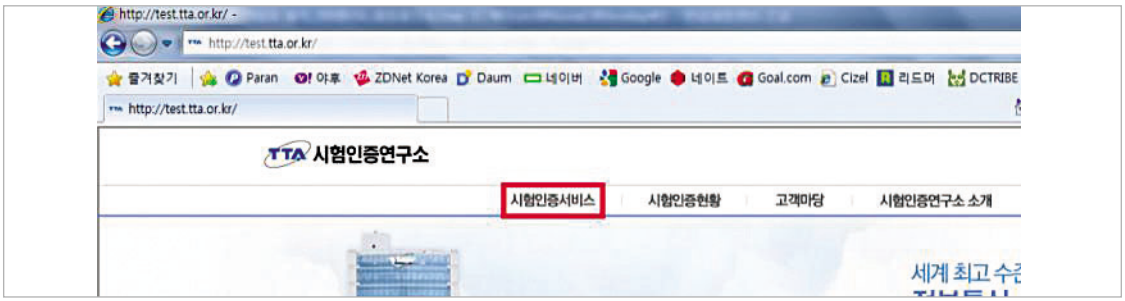
TTA 시험인증 연구소를 통해 지원 양식을 다운 받을 수 있고 또한 온라인으로 시험(인증)을 신청할 수 있다. TTA에서 진행되는 시험인증 절차는 다음과 같이 진행이 된다.

[그림 4-12] TTA Verified 시험인증 절차

TTA 시험 인증 연구소를 통하여 인증을 획득하려는 경우 홈페이지 상단 메뉴의 '시험인증현황〉 시험인증절차' 에 각 분야에 대한 신청절차가 자세하게 설명되어 있으며, 필요한 양식도 각 순서에 맞게 링크되어 있다.

① http://test.tta.or.kr에 접속하여 시험인증 서비스를 클릭한다.

[그림 4-13] TTA 시험인증서비스



② IPv6 항목을 선택하여 시험신청양식 or 온라인 시험 신청하기를 선택한다.

[그림 4-14] TTA Verified 시험인증 신청

③ 시험신청양식을 다운로드 받아서 신청할 경우 각 분야의 신청 절차에 대해 담당 안내자에게 메일을 보내면 된다.

④ 각 분야의 신청 절차에 대해 의문사항이 있으면 각 분야별 신청 안내 담당자에게 직접 문의하면 좀 더 상세한 안내를 받을 수 있다.

[표 4-13] 분야별 신청 안내

분야	전화번호	이메일
네트워크 장비분야	031-724-0134	netc@tta.or.kr
S/W 분야	031-724-0191	sqec@tta.or.kr
	02-2132-4040	sqsc@tta.or.kr
디지털방송 분야	031-724-0233	jy212@tta.or.kr
이동통신분야	031-724-0228	mctc@tta.or.kr

시험 수수료는 TTA의 근본 설립 취지에 맞게 국내 업체들에게는 적정한 할인율을 적용하고 있

으므로, 해외 시험소를 활용하는 것보다 많이 저렴하다. 시험 비용은 크게 장비 사용료 및 인건비 부분으로 구성되며, 두 가지 항목은 시험 기간과 밀접한 관련을 맺고 있다. 보통 2주정도 테스트 기간을 거친다. 그러나 시험 받고자하는 장비와 시험 종류에 따라 시험기간 및 수수료가 많이 달라지므로, 시험 기간이 일반적으로 얼마나 걸리는지는 확실하지가 않으므로 사전 협의 과정에서 시험 기간은 정해지게 된다. 테스트 완료 후 합격한 장비에 대해 해당 장비의 결과치 및 보고서, 그리고 인증서를 제공해준다.

[그림 4-15] TTA Verified 인증

4.3 CC 인증

[그림 4-16] IT보안인증사무국 홈페이지 화면

공공 · 민간기관 내부 망(엔터프라이즈망)내부의 IPv6 도입 간에 조직내 보안 요구사항 충족을 위하여 네트워크 보안장비 도입이 필수적이다. 그러나, 기존에 운용중인 IPv4기반 네트워크 보안장비로는 조직 내부적으로 송수신되는 IPv6 트래픽 안정성을 검증할 수 없다. '11년 중 IPv4 신규 주소 할당 중지 시점에 대비하여 국내 보안장비 벤더들은 IPv6기반 보안장비 개발 시 CC인증을 취득하여 시장에 보급해야만 한다.

CC 인증은 공공기관의 보안제품 도입 시 보안성 검증 기준으로 요구되는 필수조건이며, 금융권 등에서도 해당 제품의 신뢰성 검증 기준으로 적용되고 있다. CC 인증평가는 제품이나 시스템의 보안 측면을 조사하기 위해 공식적이고 엄격한 분석과 테스트 과정을 포함한다. 이러한 테스트는 포괄적이고 반복적인 과정을 거쳐 보안업체의 제품 기능을 확인할 수 있다.

국내에서는 2006년에 CCRA에 가입함으로써 명실상부한 CC 강국 대열에 들어섰다. CCRA란 국제상호인정협정(CCRA)으로 정보보호제품에 대한 평가 및 인증결과를 회원국 간에 공유하는 협정이다. 이는 정보보호제품의 인증결과를 상호 인정함으로써 국가 간에 교역 장벽을 낮추어 수출을 용이하게 하는 수단이라 할 수 있다. CCRA 가입국간 평가 및 인증 제품은 협정에 참여한 어떤 국가에서도 다시 평가를 거치지 않고 동일한 효력을 가질 수 있도록 함으로써 정보보호제품을 여러 국가에서 다시 평가해야 하는 부담감을 덜어주게 되어 글로벌 시장 형성을 촉진하게 된다.

4.3.1 CC 인증 평가 방법

평가 과정은 IT 제품의 보안 기능성과 이에 적용된 보증수단이 이러한 요구 사항들을 만족하는지에 대한 신뢰도를 확인하는 것이다. 따라서 평가결과는 소비자가 IT 제품이 그들의 보안 요구를 충족시키는지 결정하는데 도움을 줄 수 있다. 평가는 CC에 의한 방법론의 기초가 된다. 평가방법은 다음을 포함하지만 이에 국한 되지는 않는다.

① 프로세스와 절차의 분석 및 검사
② 프로세스와 절차가 적용되고 있음을 검사
③ TOE 설계 표현간의 일치성 분석
④ 요구사항에 대한 TOE 설계 표현의 분석
⑤ 증거의 검증
⑥ 설명서 분석
⑦ 개발된 기능 시험 및 제공된 결과 분석
⑧ 독립적인 기능 시험

⑨ (결함 가정을 포함한) 취약성 분석
⑩ 침투 시험

IT 제품의 보안 기능성과 평가 과정에서 그 제품들에 적용되는 보증수단에 대한 공통의 요구사항들을 제시함으로써, 독립적으로 수행된 보안성 평가의 결과들을 비교할 수 있도록 한다.

4.3.2 CC 인증 등급

평가보증등급(EAL, Evaluation assurance levels)은 해당 보증등급 획득 가능성 및 비용의 균형을 고려한 단계인 척도를 제공한다. 공통평가기준은 TOE 평가 종료 시의 보증과 TOE 운영시의 보증유지 개념을 구분한다. 공통평가기준은 TOE의 보증등급을 7 단계의 계층적인 평가보증등급으로 정의한다.

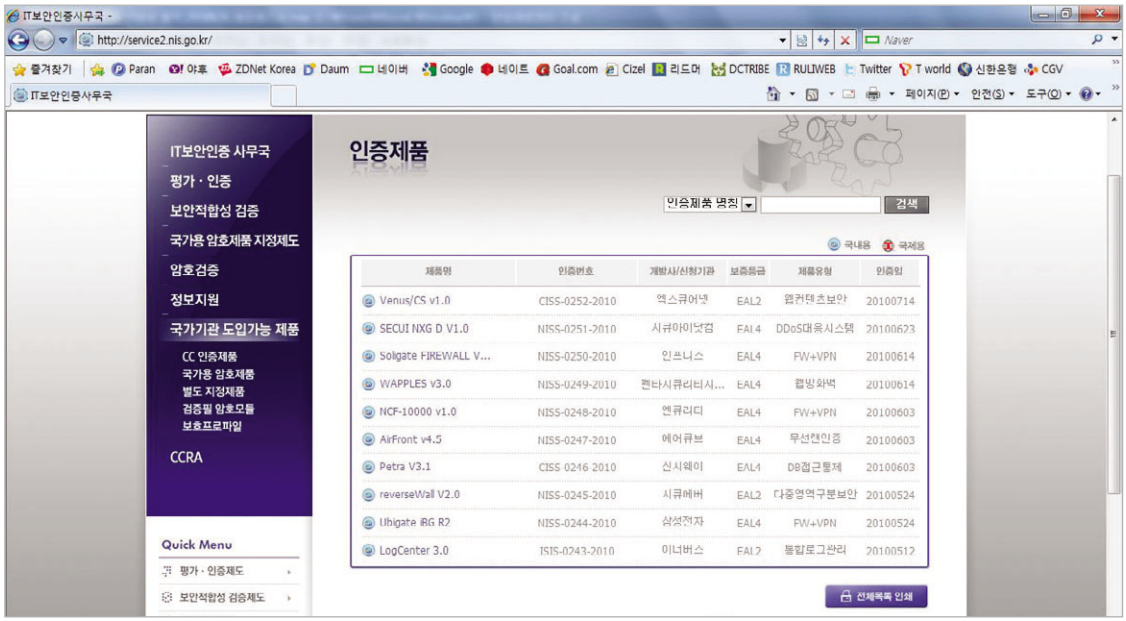
[표 4-14] CC인증 평가보증 등급

평가보증등급	시험 내역
평가보증등급1(EAL1)	기능적인 시험
평가보증등급1(EAL2)	구조적인 시험
평가보증등급1(EAL3)	체계적인 시험 및 검사
평가보증등급1(EAL4)	체계적인 설계, 시험 및 검토
평가보증등급1(EAL5)	준정형화 된 설계 및 시험
평가보증등급1(EAL6)	준정형화 된 설계검증 및 시험
평가보증등급1(EAL7)	정형화 된 설계검증 및 시험

CC 인증을 획득한 국내외 제품 리스트는 아래 주소에서 확인할 수 있다.

http://service2.nis.go.kr/

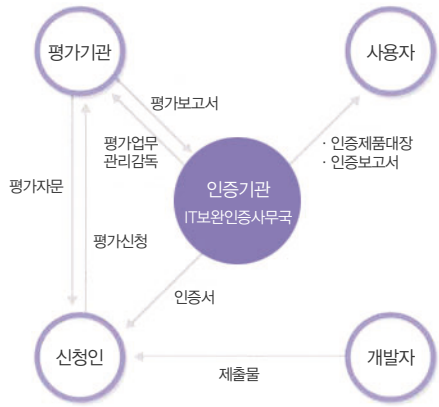
[그림 4-17] CC인증 획득 제품



4.3.4 CC 인증 절차

정보보호제품 평가 및 인증제도는 민간업체가 개발한 정보보호제품에 구현된 보안기능의 안정성과 신뢰성을 보증하여 사용자들이 안심하고 제품을 사용할 수 있도록 지원하는 제도이다. 우리나라는 1998년 2월부터 정보보호제품 평가 및 인증 제도를 시행하고 있으며 2002년부터 국제공

[그림 4-18] CC 평가 및 인증체계



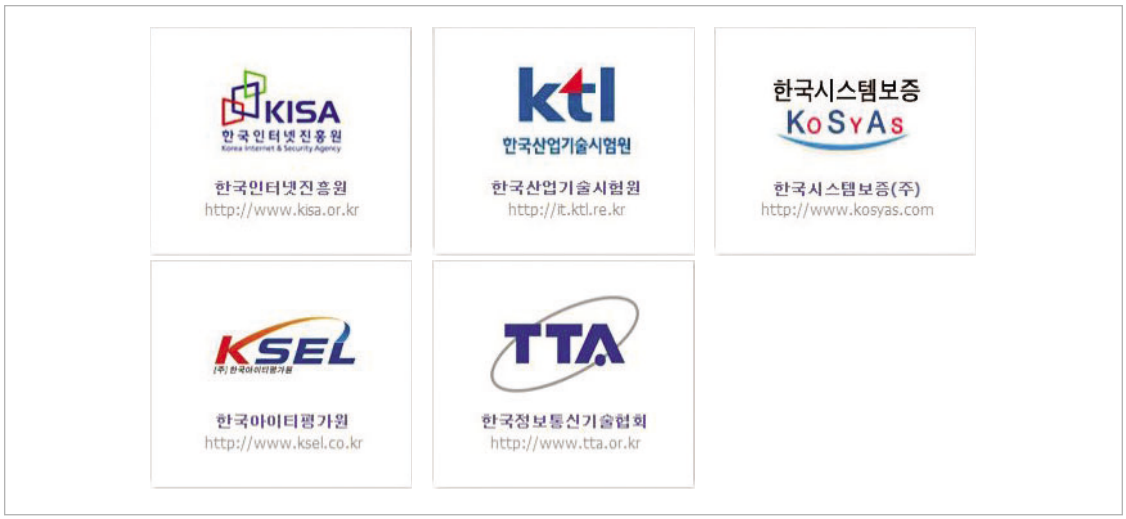
- **IT보완인증사무국**
  역할
  1. 인증업무 수행 관련 규정 제 · 개정 및 시행
  2. 인증보고서 작성 및 인증서 발급
  3. 국제상호인정협정 회원국 활동 및 관련 정책수립
  4. 평가기관의 평가업무 감독
  5. 인증제품에 대한 사후관리
  6. 인증제품대장 발간

- **평가기관**
  역할
  1. 평가업무 수행에 관한 규정 수립 및 시행
  2. 평가계약체결 및 평가 시행
  3. 평가관련 간행물 발간

통평가기준(Common Criteria)에 따라 정보보호제품을 평가 및 인증하고 있다.

CC 인증은 현재 국내 5군데에서 인증을 받을 수가 있다. 한국인터넷진흥원(KISA), 한국산업기술시험원(KTL), 한국시스템보증(KOSYAS), 한국아이티평가원(KSEL), 그리고 한국정보통신기술협회(TTA)이다.

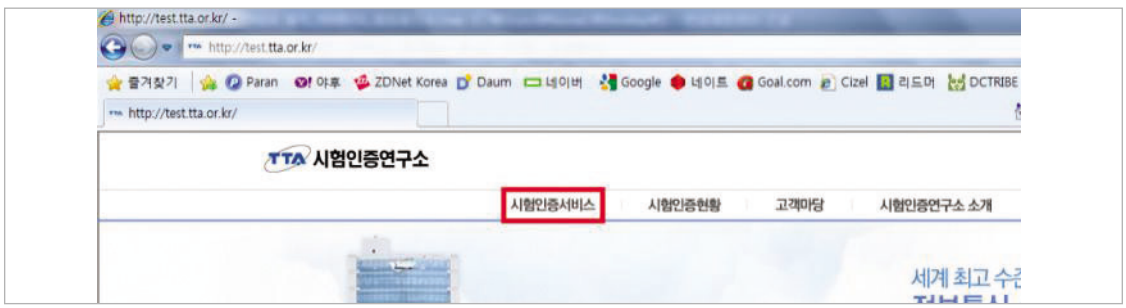
[그림 4-19] CC 평가 기관



TTA 시험 인증 연구소를 통하여 인증을 획득하려는 경우 홈페이지 상단 메뉴의 '시험인증현황〉시험인증절차' 에 각 분야에 대한 신청절차가 자세하게 설명되어 있으며, 필요한 양식도 각 순서에 맞게 링크되어 있다.

① http://test.tta.or.kr 에 접속하여 시험인증서비스를 클릭한다.

[그림 4-20] TTA 시험인증서비스 선택



② 시험/인증별 항목에서 CC 평가 및 컨설팅 항목을 선택한 후 평가 신청서를 다운받아서 작성한다.

[그림 4-21] CC 평가 신청서

③ 작성 후 CC 평가 담당자에게 우편으로 접수한다. 직인이 찍히는 부분이 있어서 우편으로 접수하는 것이 더 수월하다. 만약 단독 신청이 아니라 2개 이상의 그룹이 같이 신청할 경우 공통신청기관명부 파일도 다운받아서 같이 제출을 해야 한다.

시험 수수료 및 기간은 TTA의 여러 인증들하고는 조금 차이가 있다. 기본적으로 설립 취지에 맞게 국내 업체들에게는 적정한 할인율을 적용하고 해외 시험소를 활용하는 것보다 많이 저렴하다. CC 인증은 기본적으로 최소 3개월 동안 테스트가 진행된다. 시험 비용은 크게 장비 사용료 및 인건비 부분으로 구성되며, 두 가지 항목은 시험 기간과 밀접한 관련을 맺고 있다. 즉, 해당 장비를 얼마나 많은 요소들에 대해 얼마나 오랫동안 시험하는지의 여부가 비용을 결정하는 큰 요소로 작용하므로 일률적인 시험 비용을 산정할 수 없으며, 각 항목별 기준비용을 산정해 놓고 투입되는 Resource를 고려하여 시험 비용을 책정한다. 테스트 완료 후 합격한 장비에 대해 해당 인증서를 제공해준다.

[그림 4-22] 국내 및 국제 CC 인증

제5장
결언

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

우리는 다소 늦었지만 틈새를 공략해 국산제품을 많이 사용하는 L2 스위치, 보안장비 및 소프트웨어 위주로 IPv6를 준비하면 관련시장에 충분히 대응 가능할 것이다. 현재까지는 국내에서의 수요촉발은 신규서비스 위주로 발생할 것으로 예상되나 이미 중국, 일본 등 인구수나 기술적 우위를 선점에 관심이 많은 국가들에서 공격적으로 IPv6적용에 나서고 있어 해외시장의 제품 수요도 주시할 필요가 있다.

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

예를 들어 리거시 망의 전환을 쉽게 해주거나, IPv4/IPv6 듀얼 환경 운영에 따른 복잡성을 줄여주는 관리툴의 개발, 새로운 보안툴의 개발 등이 있을 수 있다.

수요자와 공급자 모두 서로 눈치만 보고 있는 상황에 너무 익숙해져 있는것은 아닌지 되돌아보면서 기존 제품의 업그레이드와 새로운 IPv6 지원 제품을 모색해 볼 때이다.

아울러 제품 개발과 함께 관련된 국내외 인증을 획득한다면 IPv6 시장 초기에 신뢰성 향상 등 다양한 이점을 얻을 수 있을 것이다.

이미 수 년 전부터 공공부문을 중심으로 제품 도입시 IPv6 요구사항은 지속적으로 반영되어 왔다. IPv6 적용 시점을 대비한 조치였다. IPv4 주소 할당이 중단되는 시점부터는 이러한 요구가 보다 강화될 것이다. 실제 분야별로 IPv6 적용을 검토하게 되면 테스트베드 운영, 망 구축 등 다양한 사업이 추진될 것이다. 따라서 제품 제조사도 본 책자의 타 이해관계자들의 내용도 확인하면서 IPv6에 대한 지속적인 관심과 노력을 보인다면 새로운 시장 수요에 적절히 대응가능할 것이다.

[참고문헌]

구분	내용	출처
1	IPv6 보급 촉진 기본계획	정보통신부, 2004. 5
2	IPv6 보급 촉진 기본계획 II	정보통신부, 2006. 12
3	IPv6 적용 콘텐츠 활성화 방안연구	한국인터넷진흥원, 2008, 11
4	2007년 IPv6 기술워크숍 "공공기관 IPv6 도입 실태 조사"	한국정보사회진흥원, 2007.10.12
5	공공기관 IPv6 적용 안내서	한국인터넷진흥원, 2010.3
6	공공기관을 위한 IPv6 도입 전략 수립 지침서	한국전산원, 2004. 12
7	서비스 프로바이더 및 최종 사용자를 위한 IPv6 서비스 제공 및 이용방안에 대한 연구	건국대학교, 2005. 12
8	IPv4/IPv6 전환 실무자 지침서 (프로그래밍 가이드, 전환기술, 방화벽)	한국전산원
9	IETF 표준화 동향	표준연구센터 u-인프라표준 연구팀 박정수, 2010.2.3
10	웹호스팅 업체의 IPv6 전환 가이드	한국인터넷진흥원
11	IPv6 거점 네트워크 구축 시범사업	한국인터넷진흥원, 2009. 12
12	민간부문 IPv6 도입 계획(안)	한국인터넷진흥원, 2009. 11
13	"IPv6 Rapid Deployment (6RD) in broadband networks"	http://www.cisco.com
14	한국정보통신기술협회	http://www.tta.or.kr/
15	한국인터넷진흥원 IPv6 포탈홈페이지	http://www.vsix.net/
16	IPv6 Ready Logo	http://www.ipv6ready.org/
17	Google IPv6 Implementors Conference	http://sites.google.com/site/ipv6implementors/2010/agenda
18	IETF 표준화 동향	http://www.ietf.org/

[용어정리]

용어	약어	내용
ALG	Application Level Gateway	IPv6 Translation 기술에서 동적으로 주소를 할당하고 변환하기 위해서는 응용(HTTP,DNS,SIP)에 따라 추가적인 요구사항이 발생하는데, 이를 지원하기 위하여 ALG(Application Level Gateway)를 사용.
BIND	Berkeley Internet Name Daemon	BIND는 대부분의 BSD 유닉스 계열이나 Linux 시스템에서 사용할 수 있도록 개발된 DNS로써 도메인을 IP로 매칭하는 서비스 라이브러리.
CPE	Customer Premises Equipment	통신서비스 제공 회사가 공급하여 해당 회사의 네트워크에 연결되어 있는 종단 장치로 단말기, 케이블 모뎀, adsl 모뎀 등이 있음.
DBMS	Database Management System	데이터베이스를 구성하고 이를 응용하기 위하여 구성된 소프트웨어 시스템. 사용자나 응용 프로그램이 데이터베이스를 쉽게 이용할 수 있도록 해 준다.
DHCP	Dynamic Host Configuration Protocol	TCP/IP 통신을 실행하기 위해 필요한 IP 주소 등 설정 정보를 자동적으로 할당 및 관리하기 위한 통신 규약.
DOCSIS	Data Over Cable Service Interface Specifications	HFC 망에서 케이블 모뎀 서비스를 위한 국제기술규격.
DS-Lite	Dual-Stack Less IPv6 Enabled	IPv4 islands를 IPv6 망을 통해 연동하는데 사용하는 터널 기술.
DNS	Domain Name Server	특정 네트워크에 속한 특정 호스트에 접속하기 위해 일일이 숫자로 된 IP 주소를 기억하지 않고 도메인 네임만으로도 사용 가능하게 하기 위하여 도메인 네임을 IP 주소로 전환시켜 주는 시스템.
Exchange	-	미국 마이크로소프트사가 개발한 그룹웨어 소프트웨어. 윈도즈 NT상에서 가동하는 'Exchange Server'를 서버 소프트웨어로하고, 클라이언트로는 MS 윈도즈의 표준 장비가 된 'Exchange'가 이용될 수 있다.
Firewall	-	외부의 침입으로부터 자사의 네트워크를 보호하기 위하여 게이트웨이에 설치되는 접속 장치나 기능.
FreeBSD	-	NetBSD와 함께 BSD계의 PC-UNIX. 미국 캘리포니아 대학교 버클리 캠퍼스(UCB)의 윌리엄 · 린 조리츠 교수부부가 개발한 운영 체계(OS). 386 BSD가 기본으로 되어 있다.
GUI	Graphical User Interface	도형의 형태로 화면에 표시되는 아이콘(icon)을 지정하거나 메뉴 항목 목록 중에서 메뉴를 선택함으로써 명령을 선택하고, 프로그램을 기동하며, 파일 목록을 열람하고 기타 선택을 하면서 작업을 진행하는 상호작용방식이다.
HFC	Hybrid Fiber Coax	동축 CATV 전송 망의 주요 트렁크 부분을 광케이블로 개선시킨 망.
H.323	-	서비스 품질이 보증되지 않은 구내 정보 통신망(LAN)에서의 음성, 영상, 데이터 통신의 단말 규정.
IETF	Internet Engineering Task Force	인터넷 아키텍처 위원회(IAB) 산하의 조직으로 인터넷의 운영, 관리 및 기술적인 쟁점 등을 해결하는 것을 목적으로 망 설계자, 관리자, 연구자, 망 사업자 등으로 구성된 개방된 공동체.

용어	약어	내용
IIS	Internet Information Server	미국 마이크로소프트사가 개발한 인터넷/인트라넷용 서버 소프트웨어. 버전 2.0부터 윈도즈 NT 서버에 표준으로 첨부되어 있다. 운영 체계(OS)와 통합된 것으로 복잡한 절차 없이 월드 와이드 웹 서버를 관리할 수 있다.
IPTV	Internet Protocol TeleVision	VoD, T-커머스, 오락, 뱅킹, 정보, TV 포털 및 다채널 방송서비스와 같은 멀티미디어 콘텐츠를 ADSL, FTTH와 같은 초고속 인터넷 망을 통해 디지털 셋톱박스에 연계된 TV 단말기를 이용하여 패킷방식으로 제공되는 양방향 TV 서비스를 말한다.
IPv4	Internet Protocol version 4	현재 널리 사용되고 있는 버전 4 인터넷 프로토콜. 1981년에 발간된 IETF RFC791로 문서화 되어 있다. IPv4는 211.253.131.255와 같은 점-숫자 표기의 32-bit 주소 체계로 되어있다.
IPSec	Internet Protocol Security	네트워크 계층인 인터넷 프로토콜에서 보안성을 제공해 주는 표준화된 기술로 데이터 송신자의 인증을 허용하는 인증 헤더 (AH)와, 송신자의 인증 및 데이터 암호화를 함께 지원하는 ESP (Encapsulating Security Payload) 등 두 종류의 보안 서비스 등이 있으며, IPv4에서는 선택으로 IPv6에서는 필수로 제공하도록 되어 있다.
IPv6	Internet protocol version 6	IP 주소 공간으로써 128비트를 기본으로 하며, IPv4 주소 고갈에 대비한 차세대 인터넷 프로토콜.
ISP	Internet Service Provider	일반 사용자나 기업체, 기관, 단체 등이 인터넷에 접속하여 인터넷을 이용할 수 있도록 해주는 사업자.
LINUX	-	1991년 핀란드 헬싱키 대학 학생이던 리누스 토발스(Linus Tovals)가 대형 기종에서만 작동하던 운영 체계인 유닉스를 386 기종의 개인용 컴퓨터(PC)에서도 작동할 수 있게 만든 운영 체계. 인터넷을 통하여 무료로 배포되고 있다.
KREONET	Korea Research Environment Open Network	국내 대학 및 연구 기관 대상 연구망.
KOREN	KOrea advanced REsearch Network	광대역 통합 연구 개발망.
Middleware	-	주로 상하관계나 동종관계로 구분할 수 있는 프로그램들 사이에서 매개 역할을 하거나 프레임워크 역할을 하는 일련의 중간 계층 프로그램.
MTA	Message Transfer Agent	다른 메시지 전송 에이전트(MTA)로부터 전송되어 온 메시지를 수신 측 사용자의 UA로 배송하거나, 수신 측 UA가 직접 수신하지 않을 때에는 메시지 저장 장치(MS)에 저장하여 추후에 검색할 수 있게 한다.
MUA	Mail User Agent	메일을 보내고 받을 때 이용하는 프로그램으로 메일 클라이언트라고도 한다.
NAT	Network Address Translation	사내의 비공인 주소와 공인 IP 주소를 상호 변환하는 기능.
NFS	Network File System	구내 정보 통신망(LAN) 등 정보 통신 네트워크에 접속되어 있는 다른 컴퓨터의 파일이나 파일 시스템을 공용으로 사용하기 위한 분산 파일 공유 시스템 소프트웨어.
NMS	Network Management System	망 관리 프로토콜(SNMP)을 사용하여 망을 구성하는 라우터(router), 스위치(Switch) 등 각 장비를 감시/제어하는 소프트웨어.

용어	약어	내용
Oracle	–	미국 오라클사의 관계 데이터베이스 관리 시스템(RDBMS)의 이름. 유닉스 환경에서 사용되는 RDBMS로는 현재 가장 널리 사용되는 대표적인 제품의 하나이다.
Packet	–	데이터 전송에서 사용되는 데이터의 묶음.
Proxy	–	컴퓨터나 네트워크의 중간에서 대리로 통신을 수행하는 장치나 기능.
Ready Logo	–	IPv6 포럼이 IPv6 Logo Committee를 구성하여, IPv6 장비의 신뢰성 확보 및 기술보급을 위해 2003년 9월부터 시행 중인 인증제도.
Router	–	네트워크 간의 연결점에서 패킷에 담긴 L3 IP 정보를 분석하여 적절한 통신 경로를 선택하고 전달해 주는 장치.
Sendmail	–	가장 일반적으로 사용되고 있는 간이 전자 우편 전송 프로토콜(SMTP) 소프트웨어.
SIP	Session Initiation Protocol	IETF에서 개발한 IP 전화 통신 신호 프토로콜. 주로 IP 호출을 통한 음성에 사용되며 비디오나 미디어 유형에 사용할 수도 있다.
SNMP	Simple Network Management Protocol	TCP/IP의 망 관리 프로토콜(RFC 1157). 라우터(router)나 Switch 등 망 장비(network agent)의 망 관리 정보를 망 관리 시스템에 보내는 데 사용되는 표준 통신규약.
Solaris	–	선 마이크로시스템즈사의 유닉스 운용 체계 버전. 운용 체계는 물론 자바 프로그램을 실행하는 자바 가상 머신, 유닉스의 그래픽 사용자 인터페이스(GUI) 규격의 CDE/Desktop과 네트워킹 프로그램을 포함한다.
SSH	Secure Shell	보안 등급이 낮은 네트워크상에서 보안 등급이 높은 원격 접속 개시나 데이터 전송을 실현하는 규약.
Telnet	–	호스트와 단말 간 또는 호스트와 호스트 간에 가상 단말 통신 기능을 행하기 위한 절차를 제공하여, 네트워크상의 한 시스템 사용자가 자기 시스템(로컬 시스템)의 자원에 접속하는 것처럼 다른 시스템(원격지 시스템)에 접속할 수 있게 한다.
TFTP	Trivial File Transfer Protocol	파일 전송 규약(FTP)보다 사용은 단순하나 기능이 미약한 파일 전송용 인터넷 소프트웨어.
Tunneling	–	하위층 통신 규약의 패킷을 상위층 통신 규약으로 캡슐화하는 것으로, 통신망 상의 두 점 간에 통신이 된다.
VOD	Video On Demand	프로그램을 주문하고 기다려야 하는 기존의 PPV(Pay Per View) 서비스와는 달리 가입자가 원하는 시간에 원하는 프로그램을 즉시 선택해 시청 할 수 있는 양방향 영상서비스.
VPN	Virtual Private Network	공중망 상에 사설망을 구축하여 마치 사설 구내망 또는 전용망 같이 이용하는 통신망.
VoIP	Voice over Internet Protocol	PSTN 네트워크를 통해 이루어졌던 음성 서비스를 IP(Internet Protocol)기술을 사용하여 제공.

용어	약어	내용
Wi-Fi	Wireless-Fidelity	2.4GHz대역를 사용하는 무선 랜(WLAN) 규격(IEEE 802.11b)에서 정한 제반 규정에 적합한 제품에 주어진 인증 마크.
WWW	World Wide Web	세계 규모의 거미집 또는 거미집 모양의 망이라는 뜻으로, 하이퍼텍스트(hypertext)라는 기능에 의해 인터넷상에 분산되어 존재하는 온갖 종류의 정보를 통일된 방법으로 찾아볼 수 있게 하는 광역 정보 서비스 및 소프트웨어.
6NGIX	IPv6 Next Generation Internet eXchange	국내외의 ISP 대상으로 IPv6 망 연동을 제공.
6KANet	IPv6 Korea Advanced Network	국내 공공기관 및 연구기관 등에 IPv6 인터넷 서비스를 제공하는 IPv6 가입자 망.
6RD	IPv6 Rapid Deployment	RFC5969 6to4 Tunnel 기반 기술.
6to4		RFC3056, Router to Router Tunnel 기술.

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〉〉