2008-13 | 연구보고서

전국 경찰전화망 고도화 방안 연구

치안정책연구소
POLICE SCIENCE INSTITUTE

연구보고서 2008-13

전국 경찰전화망 고도화 방안 연구

≪研 究 陣≫

연 구 위 원 : 이 인 화 (씨에스티)

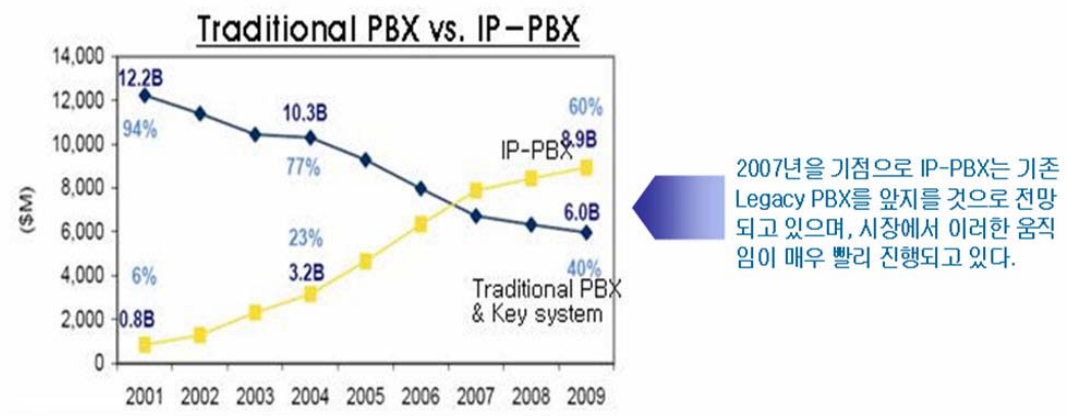
목 차

제1장 서 론

제1절 연구의 배경 및 목적

IT839로 추진되던 VoIP(인터넷전화)는 2005년 말부터 본격적인 상용서비스를 개시하였으며 이와 함께 기존 TDM 기반의 PBX를 IP-PBX가 빠른 속도로 대체하고 있는 추세이다.

〈그림 1〉 전 세계 PBX(TDM)의 IP-PBX로의 전환 추이도



출처 : Xener

특히 2006년부터는 인터넷 주소 고갈에 대비하여 정부 중심으로 신 인터넷 주소체계(IPv6) 기반 VoIPv6서비스가 확산되고 있다. 또한, 정부의 u-Korea 정책 및 RFID/USN 확산 등 본격적인 유비쿼터스(Ubiquitous) 사회 진입을 위한 IT 신기술 사업 확대가 가속화됨에 따라 경찰 치안환경도 모든 전자적 처리가 통합, 융합되어 가고 있으며, 모든 교환 체계가 IP교환기로 통합됨에 따라 경찰도 미래 사회 대비를 위해 경찰 전화망 고도화가 필요하다.

따라서, 본 보고서에서는 경찰 전화망을 PSTN기반 전화망에서 VoIPv6망으로 고도화를 위한 IP 주소체계를 IPv6기반으로 설계 하여 체계적인 IPv6 주소 체계를 정립하고, PSTN 전화망 구조의 번호체계를 ALL-IP기반의 VoIPv6 환경에 적합하도록 개선 방안을 연구하여 제시하는데 목적이 있다.

제2절 연구 범위

전국경찰전화망이 All-IP기반 환경으로 고도화됨에 따라, 이에 부합하는 전화 번호체계 개선 및 새로운 IP 주소체계의 설계가 필요하다.

따라서, 향후 All-IP기반 전국전화망 구축을 위해 보안성, 상호 호환성, 연동성을 고려한 전화번호 체계 및 새로운 IP 주소체계를 설계에 대한 연구 범위를 다음과 같이 선정하였다.

◎ **현황 분석**

- 경찰전화 시스템 현황
- 경찰전화 번호체계 현황
- 경찰 IP 네트워크 구조

◎ **환경 분석**

- IPT 기술 및 동향 분석
- IPv6 기술 동향 분석
- 타 기관 IPT 도입 및 VoIP 번호체계 설계 사례
- 타 기관 IPv6 도입 및 IPv6 주소 설계 사례

◎ IPv6 **도입**

◎ VoIP **번호 체계 설계**

◎ 경찰통신망 보안

◎ 기타 고려사항

◎ 결론

2장에서는 경찰전화망의 현황 파악하고, 3장에서는 환경 분석을 통하여 IPT/VoIP, IPv6의 핵심 이슈를 도출하고 4장에서는 IPv6 도입에 관련된 내용과 IPv6망 주소 할당 방안을 제시하고, 5장에서는 VoIP 번호체계 설계 이슈와 VoIPv6 번호체계 설계(안)을 제시하고, 6장에서는 경찰 전화망 보안서비스 제공 방안을 제시하고, 7장에서는 기타 고려사항에 대한 내용으로 단말과 품질이슈와 대안을 제시한다. 마지막으로 8장에서는 본 보고서에 대한 결론을 짓고 향후 나아갈 연구 방향을 제시하겠다.

제2장 경찰전화망 내부 현황 분석

제1절 시스템 현황

현재 시스템은 본청, 지방청, 경찰서, 직할대, 학교 별 개별적 PBX 보유하고 있으며 각각의 PBX는 수직적으로 음성 전용선(E&M 2wire)을 이용하여 연동하고 있다. 다음 〈표 1〉은 전국 경찰 교환기 수량 및 전화기 설치 현황을 보여준다.

〈표 1〉 전국 경찰 교환기 수량 및 전화기 설치 현황

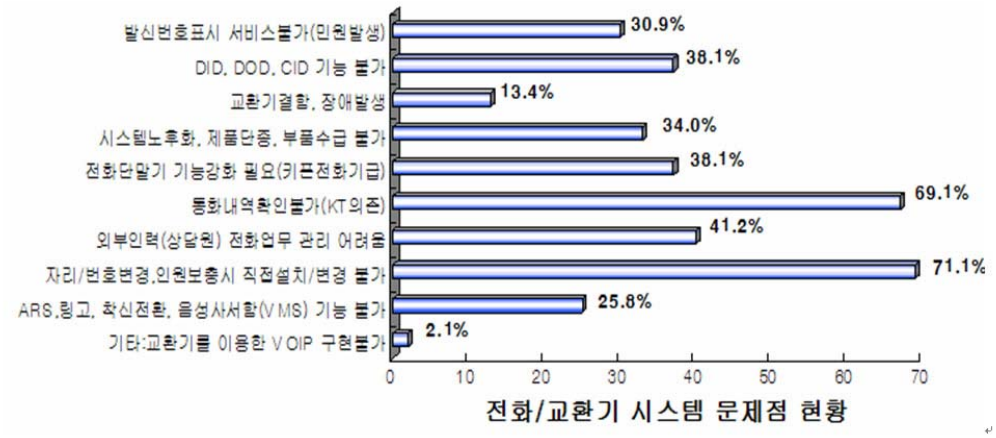
구 분	교환기 수량	전화기 설치 현황
본 청	1	2,500
지방청	14	12,822
경찰서계	235	64,090
직할대계	12	3,166
학 교	3	1,133
계	256	83,711

출처 : 전국 경찰 전화망 고도화 방안 연구 보조 자료 <2007.5.10>

각각의 PBX는 본청을 중심으로 수직 연동되어 있기 때문에 이로 인한 PBX간 연동 딜레이 및 추가적인 액세스코드가 필요하다. 그리고, PBX간 2W E&M (2 wire Ear and Mouse)의 아날로그 신호방식을 사용한다. 이 E&M 신호방식을 사용하기 때문에 발생되는 연동 딜레이가 경찰전화망의 수직 구조로 인해 타 지구대간 통화 연결 시간이 수 초가 발생하게 된다. 또한 수직적 구조 문제로 인한 불필요한 PBX가 늘어 남과 동시에 회선 비용 증가로 비용적 부담이 크다. 따라서 수직적인 계층 구조를 단순화 시키고, 본청 및 지방청 중심의 수평적이 구조를 가지게 함과 동시에 액세스코드 및 회선의 비효율적인 부분을 개선하여야만 한다.

다음 〈그림 2〉는 Legacy PBX 시스템의 문제점을 나타낸 것으로 부가서비스, 시스템 노후화, 유지보수 등에 여러 가지 문제점을 가지고 있다. 특히 자리/번호변경 시 직접변경이 어렵고, 자체적으로 통화내역을 확인할 수 없다.

〈그림 2〉 Legacy PBX 시스템의 문제점



제2절 음성전용선 및 팩스현황

아래의 〈표 2〉는 현재 사용 중인 음성전용선 및 팩스 현황 보여준다.

〈표 2〉 음성전용선 및 팩스현황

구 분	음성 전용선	모사전송기(FAX)
본 청	330회선	317
지방청	3,000회선	1,465
경찰서계	8,700회선	6,606
직할대계	4,500회선	275
학 교		39
계		8,702

출처 : 전국 경찰 전화망 고도화 방안 연구 보조 자료 <2007.5.10>

Data 전용선과 음성 전용선을 분리하여 사용함으로써 고가의 회선비용 및 운용비용이 지출되고 있다. 또한, 음성 전용선과 FAX의 대수를 비교해봤을 때 주로 팩스를 사용하는 용도로 전용선이 쓰이고 있다.

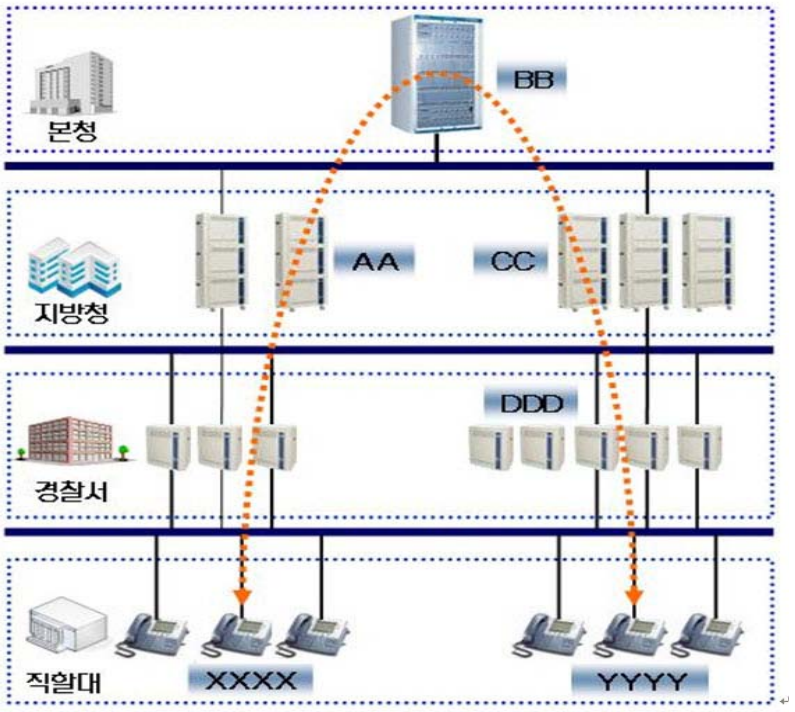
제3절 전화번호 체계(Numbering Plan)

아래의 〈그림 3〉는 경찰청 전화번호 체계 및 호가 라우팅되는 것을 나타낸 것으로, 직할대 "XXXX"에서 타 지역 직할대 "YYYY"로 전화를 거는 예이다. 통화가 이루어지기 위해서는 경찰서→지방청→본청→지방청→경찰서→지구대 거쳐야만 한다.

"XXXX"에서 "YYYY"로 전화를 걸기 위해서는 우선 자체 키폰 시스템을 통하여 경찰서 교환기를 거쳐야 하고, 이후 지방청, 본청의 교환기를 거친 이후 "YYYY" 지역의 지방청, 경찰서 교환기를 거쳐야지만 "YYYY"에게 호가 전달된다. 중간에 호가 라우팅되는 경찰서, 지방청, 본청을 경유할 때마다 액세스코드가 붙으므로, 실제 전화번호는 AA-BB-CC-DDD-YYYY가 된다.

이와 같이 서로 다른 권역의 경찰서 간 통화 시 액세스코드를 사용하는데, 최대 13자리 전화번호를 사용하고 있다.

〈그림 3〉 전화번호 체계(Numbering Plan)



출처 : 전국 경찰 전화망 고도화 방안 연구 보조 자료 <2007.5.10>

1. 교환국 번호 및 내선번호 체계

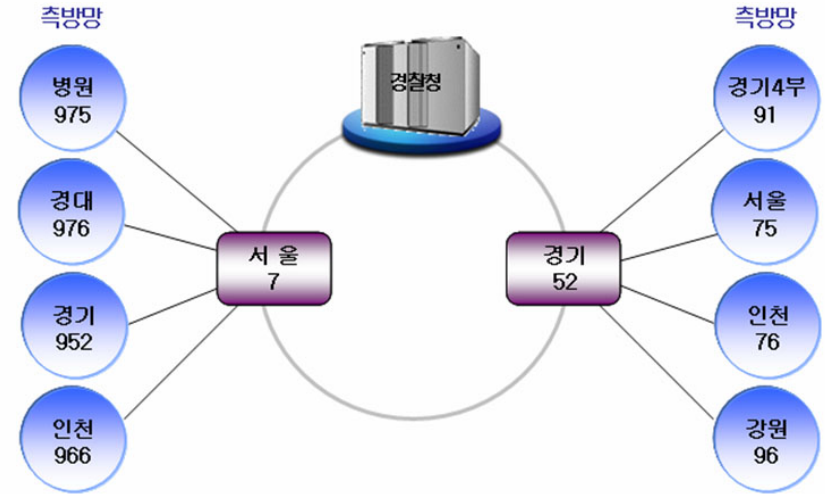
현재 번호체계의 구조는 경찰청을 중심으로 지방청, 경찰서, 직할대 순으로 계층화 되어 있으며, 각각의 교환국은 한자리 이상의 액세스 코드를 가진다. 아래의 〈표 3〉은 각 지방청 및 부속기관 등의 교환국번이다.

〈표 3〉 전국경찰 교환국번

구 분	교환국번	구 분	교환국번
경찰청	8	행자부	40-111
서울지방청	7	면허단	47
지방청	50~60	수보연	48
인천지방청	66	해 경	49
중 앙	63	경찰대학	61
국과수	64	종 합	62
병 원	65		

경찰서의 경우 일정한 패턴으로 설계되어 있지만, 지방청 및 측방망의 경우 추가되는 부분을 고려한 설계가 이루어지지 못했다. 특히 측방망은 연계가 필요한 지방청간 또는 지방청과 부속기관 등이 경찰청 교환기를 거치지 않고, 직접 연계하고 있으나, 각각의 지방청의 교환국번의 설계가 각 지방청 교환기 위주로 설계 되어 전체적으로 일정한 패턴이 없고, 자릿수가 일정하지 않다.

〈그림 4〉 측방망 교환국번 비교(서울 vs. 경기)



위의 〈그림 4〉은 서울 지방청에서 연계되는 측방망의 교환국번과, 경기 지방청에서 연계된 교환국번을 비교한 것으로 번호 체계가 상이함을 보여준다. 단일 PBX에서는 일정한 패턴을 가지고 있으나, 전체적인 측방망 교환국번 적용에 있어서는 일정한 적용 규칙이 없다. 따라서 측방망 번호체계에 대한 일괄성 있는 정책이 필요하다.

아래의 〈표 4〉는 전국 경찰의 기능별 공통 내선번호이다. 경찰청 및 지방청의 경우 4자리의 내선번호를 사용하고 있으며, 경찰서는 3자리 내선번호를 사용한다. 직위별 및 업무 분류에 따라 2*** 또는 2** 패턴을 사용한다.

〈표 4〉 기능별 공통 전화번호

구 분	경 찰 청	지 방 청	경 찰 서	비 고
청장(서장)	2010	2010	210	
1 차장	2011	2011		
2 차장		2012		
총무과장	2021			
경무기획국장	2001			
경무부장(과장)		2020	220	
생활안전국장(부•과장)	2045	2045	245	
수사국장(부•수사과장)	2065	2065	265	
형사과장	2070	2070	270	
경비교통국장(과장)	2055	2055	255	
교통지도부장(과장)		2050	250	
정보국장(부•과장)	2080	2080	280	
보안국장(부•과장)	2090	2090	290	
홍보관리관	2013	2013		
감사관(청문감사관)	2016	2016	216	
정보통신관리관(과장)	2040	2040		
외사국장(과장)	2075	2075		

경찰서 공통 내선번호의 경우 기능별 공통 전화번호를 제외하고는 적용형태가 일정치 않다. 체계적으로 부서별 또는 업무별, 직위별로 구분할 수 있도록 내선번호의 개선이 필요하다.

〈표 5〉 경찰서 공통 내선번호

실과명	번호	실과명	번호	실과명	번호
서장	210	생활질서계	345	작전	261
〃 댁	310	방법술찰대장	348	상황실	229
부속실	211	순찰대	354	정보과장	280
청문감사관	216	여성청소년계장	248	정보1계장	281
경무과장	220	여성청소년	348	정보1	381
경무계장	221	수사과장	265	정보2계장	282
경무	321	수사지원팀	366	정보2	382
경리계장	222	형사과장	270	보안과장	290
경리	322	형사지원팀	371	보안1계장	291
〃	323	교통과장	250	보안1	391
민원실장	224	사고조사계장	251	보안2계장	292
민원실	324	사고조사	351	보안2	392
〃	325	지도계장	252	외사계장	276
정보통신계	241	지도	352	외사	376
〃	341	뺑소니수사전담	254		
전자교환기실	200	경비과장	255		
생활안전과장	245	경비작전	256		
생활안전계장	246	경비	257		
생활안전계	346	〃	258		
생활질서계장	247				

현재 경찰의 교환국 번호 현황을 파악해본 결과, 지방청 및 부속 기관들의 추가 및 확장에 유연하게 대처할 수 있는 번호체계 및 라우팅 정책이 고려되어 설계 되지 않았으며, 측방망의 경우 각각의 지방청 별로 PBX의 정책에 따라서 번호가 부여되지만, 전체적으로 볼 때 일정한 패턴을 가지지 않는다. 이러한 측방망의 문제는 IPT기반 통신망으로 진화함에 따라 자연히 해소될 것이다.

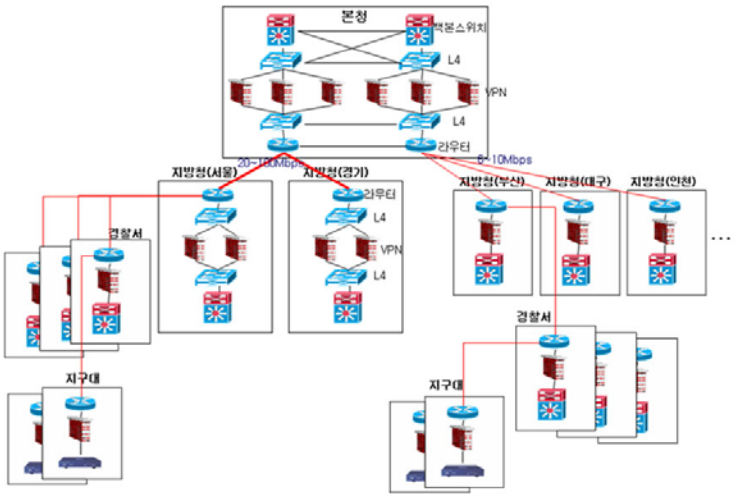
2. 호 라우팅 체계

경찰청의 호 라우팅 체계는 내선 연결하는 경우와 외부 기관 및 외부 PSTN 연결로 구분된다. 각각의 PBX에서의 내선 연결의 경우 Prefix를 통한 번호 대역을 구분하고, 측방망 및 상위 연동의 경우 액세스코드로 구분된다. Prefix는 정해진 Prefix에 대해 일정한 호 라우팅을 하게 된다. 예로 부산 지방청의 경우 교환 국번 “50” 이고 측방망의 경우 울산, 경북, 경남, 제주 (“57”, “58”, “59”, “60”) 이다. 만약 “57”로 시작되는 번호가 들어오게 되면 울산 지방청 번호로 인식하고, 이 Prefix를 떼고 나머지 번호만 울산 지방청에 넘기는 방식을 사용한다. 번호가 “57 2010” 이라고 가정하면 “57”을 떼고 내선 번호 “2010”로 호가 전달된다.

제4절 경찰 IP 네트워크 구조

아래 〈그림 5〉는 현재 경찰 IP 네트워크 구조를 나타낸 것으로 본청을 기준으로 하위에 지방청을 연결하고, 각 지방청 아래에 경찰서, 지구대가 연결되는 구조를 가진다.

〈그림 5〉 경찰 IP 네트워크 구조



본청 라우터와 지방청 라우터 간의 회선은 서울과 경기 지방청은 20~100Mbps, 타 지방청은 6~10Mbps의 광 회선을 사용한다. 본청과 서울/경기 지방청은 백본 스위치와 라우터 사이에 L4 스위치 및 VPN이 위치하고, 나머지 예하 지방청과 경찰서 지구대에는 L4 스위치가 없는 형태이다.

현재 경찰 네트워크의 특징은 모든 노드에 파이어월을 사용하고 있다. 이러한 구조는 향후 다양한 망 및 서비스와의 연동이 필수적인 환경에서는 새로운 대응방안이 필요할 수 있다. 인터넷 구축사상인 Entry point 에 필터링 기능을 삽입해 폐쇄 그룹을 형성하는 기법인 CUG(Closed User Group) 형태의 기법이 필요할 것이다.

제3장 환경 분석

제1절 IPT/VoIP

1. IPT 기술 및 동향

가. IPT(Internet Protocol Telephony)의 정의

IPT(Internet Protocol Telephony)란 회선교환 방식의 전화와는 달리 인터넷 망의 근간인 IP 네트워크에 음성을 패킷 형태로 전송하는 음성 서비스로 음성과 데이터를 하나의 망으로 통합 제공함으로 망 자원이 보다 효율적으로 사용될 수 있으며, 인터넷과 연계된 다양한 지능망 서비스의 제공이 가능하다.

- 기술의 발전 및 저렴한 이용료 등으로 등장
- TDM(Time Division Multiplexer)기반이 아닌 순수 IP 기반의 음성통신 시스템으로, 네트워크에 데이터, 음성, 비디오를 실시간으로 통합하여 전달하는 기술
- 저렴한 비용을 최대 장점으로 확산 추세이며 MGCP/MEGACO를 거쳐 SIP로 발전하는 추세임

아래의 〈표 6〉에서 IPT와 PSTN를 비교 분석하였다.

〈표 6〉 IPT과 PSTN의 비교

구 분	IPT	PSTN
접근범위	인터넷이 가능한 곳	회선이 설치되어 있는 곳
통신방식	SIP으로 통일	국가별로 틀림
통신방법	패킷 음성 (Packet Voice)	음성 (Circuit Voice)
회선이용률	다수 사용자 동시 사용	한 명이 독점적 사용
통신사용료	접속 속도 및 회선 종류에 따라 다름	거리, 시간에 따라 차등
이용방법	복잡	단순

나. IP Telephony 변화

과거에는 IP 망을 경유하여 음성통화를 하는 기술에서 현재는 IP 기반의 망을 포함한 Packet 망을 경유하여 멀티미디어 서비스 (실시간 Voice, 비디오, Data)을 제공하는 Component, Protocol, Procedure를 규정하는 기술로 발전되고 있다.

다음의 〈그림 6〉는 IPT 변화를 보여준다.

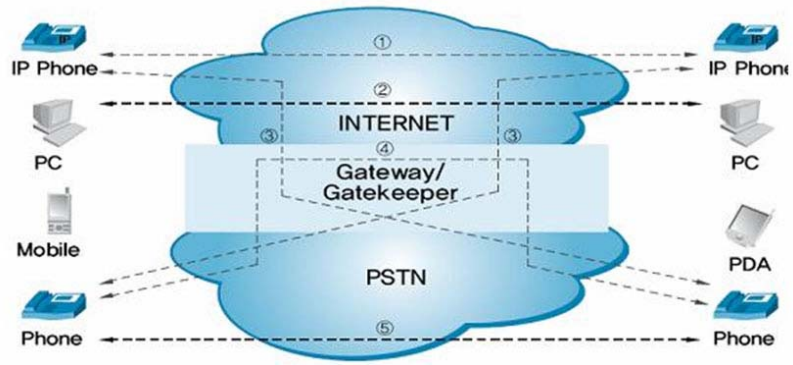
〈그림 6〉 IP Telephony 변화

- "UC"는 개인, 그룹, 조직의 생산성을 향상시키기 위한 도구로써 기업의 다양한 통신수단을 단일 플랫폼 또는 인터페이스를 이용하여 사용, 관리, 통합 제어하는 솔루션을 의미한다.

다. IPT 서비스 형태

IPT 서비스는 단말의 종류에 따라 〈그림 6〉와 같은 형태로 구분할 수 있다.

〈그림 7〉 IPT 서비스 형태



①은 “IP폰 to IP폰 서비스 이다. 이 서비스는 공중전화망을 경유하지 않고 인터넷을 통하여 IP주소와 착발신번호를 할당 받은 IP전화기들 간 음성서비스를 제공한다.

②는 “PC to PC” 서비스이다. 이 서비스는 공중전화망을 경유하지 않고 인터넷을 통하여 통신ID 또는 IP주소 등을 보유한 통신 커뮤니티 간 음성서비스를 제공한다.

③은 “IP폰(PC) to PSTN폰” 서비스 이다. 이 서비스는 인터넷과 공중전화망 (또는 무선망)을 상호 연동하여 IP주소화된 착·발신번호를 할당 받은 IP전화기와 일반 유선(무선) 전화 간 음성서비스를 제공한다.

④는 “PSTN폰 to PSTN폰” 서비스 이다. 이 서비스는 공중전화망의 일반 전화기가 인터넷을 경유하여 다른 공중전화망의 일반전화와 연결하여 음성서비스를 제공하는 서비스이며 주로 국제전화에 이용되고 있다.

⑤는 공중전화망 기반의 일반 유선전화서비스 제공이다.

라. 가입자망 구성요소

각 기관별 가입자 IPT 서비스 망은 다음과 같은 구성 요소로 이루어지며, 구성 모델에 따라 다르게 구성된다. 따라서 망 연동 및 서비스 도입 관점에서 모델을 결정할 필요가 있다.

〈표 7〉 인터넷전화 구성요소

구성요소	주요 내용
IP-PBX	호 및 세션 제어 시스템으로 Legacy PBX와 같은 역할수행 IP-Phone 및 GW(Gateway) 을 수용관리하며, Core망의 Node와 연동하는 역할 수행
IP-Phone	음성 및 영상폰이 있으며, IP-PBX와 연동하여 서비스를 제공받을 수 있는 가입자 전화기이다 SIP 프로토콜을 지원하며, Audio 및 Video Encoding/ Decoding 기능을 수행한다.
SIP-GW	FXS, FXO, PRI 회선을 제공하며, 기존 Legacy 장치(Phone, PBX) 들을 IPT망으로 수용하는 Gateway 역할을 수행. SIP 프로토콜을 지원하며, Audio Encoding/Decoding 기능을 수행한다.
VAS	Audio 및 Video Conference. VMS, IM/PS 기능을 제공하여 회의통화, 사서함서비스를 제공하고, 각 기관의 업무용 그룹웨어등과 Collaboration할 수 있는 IM/PS기능 등을 제공하는 장치
Legacy-PBX	각 기관에서 운용중인 사설교환기 아날로그폰을 수용하며, Core 망의 TDM교환기와 연동
Legacy-Phone	각 기관에서 사용자 아날로그 전화기

마. IPT의 필요성

1) U-IT839 정책에 따라 현재까지 사용하던 기간통신사업자의 PSTN (Public Switched Telephone Network)이 BcN으로 전환되어 일반전화의 IP화가 추진되고 있다.

2) 공공기관 내 정보통신 시스템이 데이터 망과 음성정보망 등을 통합적으로 지원하는 IPT 시스템 기반으로 빠르게 고도화하고 있음.

3) 중앙부처를 비롯해 정부 투자기관, 지방자치단체까지 대민 서비스 고도화와 업무 효율성을 높이기 위한 프로세서 개선 작업이 수행되면서 IP 통합관리가 가능하고 통

신비용 절감효과는 물론 재택근무 등의 활용성이 높은 IPT 시스템 기술이 각광을 받고 있는 상황임.

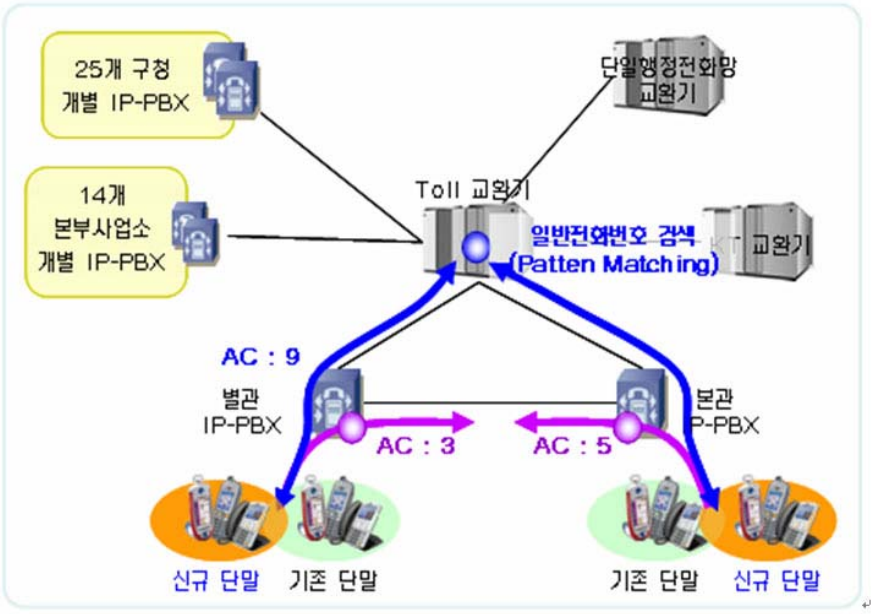
2. 타 공공기관 IPT 도입 및 VoIP 번호체계 설계 사례

경찰전화망의 IPT도입 모델 설계에 앞서 타 공공기관의 IPT도입 사례 및 번호체계 설계 사례를 분석하여, 시사점을 도출하고 경찰전화망 모델 및 번호체계 설계에 참고하고자 한다.

가. 지방 자치단체의 IPT 구축사례

아래의 그림은 지방 자치단체의 IPT 구축사례를 보여준다.

〈그림 8〉 타 공공기관 IPT 구축 사례



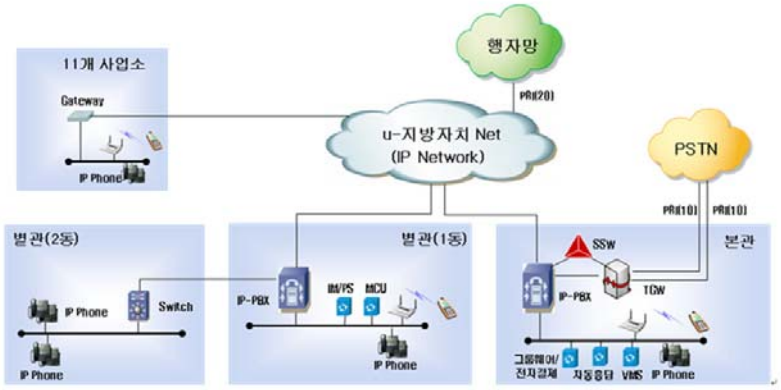
기존 PSTN 망은 Toll 교환기를 중심으로 본관과 별관 그리고 25개 구청의 PBX, 14개 본부 사업소의 PBX를 연동하는 방식이었다. 1단계 IPT도입 사업으로 각각의 구청별로 IP-PBX를 개별적으로 도입하였고, 본청의 Toll 교환기는 그대로 유지하고, 본관 PBX와 별관 PBX를 IP-PBX로 전환하였다. 또한 기존의 번호 할당의 문제점과 1인 1번호 체계 구축을 위한 번호체계를 설계하였다. 신규단말과 기존단말을 모두를 수용할 수 있는 IP-PBX 도입하고, 본관과 별관과의 통화에는 AC코드 "3", "5"을 사용하여 통화를 하고, 외부 기관 및 구청 등은 Toll 교환기를 통하여 연결되는 형태로 구축되었다. 이러한 1단계 IPT 도입형태는 2단계 때 Toll 교환기가 IP기반의 교환기로 교체 되더라도 번호체계는 그대로 유지된다.

나. 행정자치부 망과의 연동

단일행정전화망과의 연동은 기존 Toll 교환기와 연동이 이루어지지만,

행정전화망이 VoIP로 전환되면 기존의 PSTN 연동 체계에서 VoIP 연동 체계로 전환되어야 한다. 차후에 행정전화망이 PSTN기반 망에서 IP기반 망으로 전환되었을 때 이에 대한 연동부분에 대한 고려가 필요하다. 현재 ISDN(PRI 20회선)으로 행정자치부 망과 연동되어있는데, 기존 Toll 교환기에서 SSW(Soft Switch)을 통해 행자망이 IP기반 전화망으로 전환되어도 연동가능 하도록 설계되었다.

〈그림 9〉 지방자치단체 IPT 도입(All-IP)



다. VoIP 번호 할당 및 호 라우팅

기존 PSTN 기반 번호체계는 일반전화번호의 하위 4자리를 내선번호로 사용하였다. 예를 들어 “1234-5678”의 일반번호(PSTN)에서 내선번호는 “5678” 이였다. 일반전화번화와 내선번호가 일대일로 매핑되어 있기 때문에 번호 자원의 한계가 있어 1인 1번호를 가질 수 없었다.

IPT 번호 할당 및 호 라우팅은 이러한 기존의 사용자 환경인 다수의 사용자가 1대의 전화를 공유하여 쓰던 방식에서 1인 1번호 체계 형태로 추진되었다. 그리고 행정 조직 및 부서를 기준으로 한 효율적인 번호체계 정립을 위해 계층적인 번호체계를 수립하였고, 추가적인 확장 및 조직/이동에 유연하게 대처할 수 있도록 번호체계를 수립하는데 주안점을 두고 설계되었다. 아래의 2가지 방안을 기반으로 번호 설계가 이루어 졌다.

A. 방안1 : 신규 내선번호 + 기존 일반전화번호 체계

B. 방안2 : 신규 내선번호 + 신규 일반전화번호 체계

“A”안의 경우 기존 일반전화번호를 그대로 유지하여 시민고객 및 외부 사용자의 혼돈을 방지할 수 있고, 일반전화번호 확장 및 조직 변경/이동으로 인한 번호체계의 변경이 최소화 되는 장점이 있으나, 새롭게 설계된 내선번호 체계에 대한 적응이 필요하다.

“B”안의 경우 일반전화번호의 하위 4자리를 내선번호로 활용할 수 있는 장점은 있으나, 연속된 다수의 일반전화번호를 사업자로 부터 신규발급이 필요하고, 기존 Toll 및 PBX의 호 라우팅과 연동 시스템의 정책 변경이 필요하다. 그리고 기존 일반전화번호 및 내선번호가 모두 바뀌게 됨으로 인한 시민고객, 외부 및 내부 사용자의 혼돈이 발생된다.

라. 타 공공기관 사례의 시사점

위에서 지방 자치단체의 IPT 도입 및 번호체계 설계 사례들을 살펴보았다. 위의 지방청 사례에서 경찰청 IPT 구축 및 번호체계 설계에 참고할만한 사항은 다음과 같다.

첫째, IPT 도입에 있어서 경찰청과 유사하다. 각 구청은 자체적으로 IP-PBX를 도입하였고, 본관 및 별관 또한 IP-PBX를 도입함으로써 내부 IPT 환경을 구축하였다. 또한

타 기관 및 구청등과의 단순하면서도 편리한 연계를 위해 단일 연동 포인트 장비인(Toll 교환기)을 통한 연동 체계를 구축하였다.

둘째, IPT 전환에 따른 1인 1번호 체계 도입하기 위해 기존 번호체계를 IPT기반 번호 체계로 설계하여 추가 확장 및 조직/이동 변경에 유연한 번호 체계를 구축하였다.

셋째, 번호설계에 있어서 기존 번호체계를 최대한 유지하여 시민고객의 불편을 최소화 하고, 신규 내선번호 체계를 도입함으로써 추가 확장에 대응할 수 있는 방향으로 설계가 이루어졌다.

3. IPT, VoIP 벤더 동향

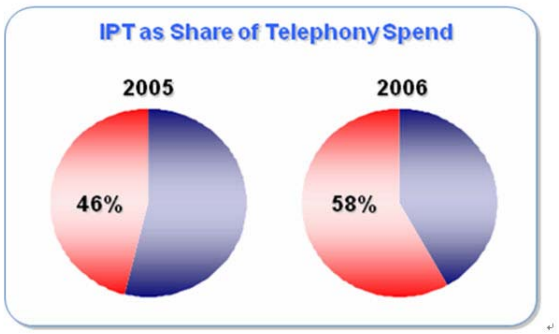
가. 해외 Telephony 시장 점유율 및 SIP 기술 동향

최근의 IPT가 급격하게 Telephony 시장을 장악해가고 있다. 특히, VoIP 통신프로토콜의 하나인 SIP가 IPT의 핵심기술로 부각되고 있다.

본 장에서는 해외 IPT 및 VoIP 벤더들의 추세를 통해 최근 Telephony 시장동향 및 SIP의 기술현황을 파악하고자 한다.

〈그림 10〉은 IPT가 미국 Telephony 시장의 점유율을 나타낸 것으로 시너지 리서치 그룹에 의하면, 2005년에 46%에서 2006년 58%로 비중이 높아 졌음을 나타낸다. 특히 엔터프라이즈들은 IPT가 전체 전화통신비를 절반 이하로 줄일 수 있는 새로운 전환점으로 보고 있다.

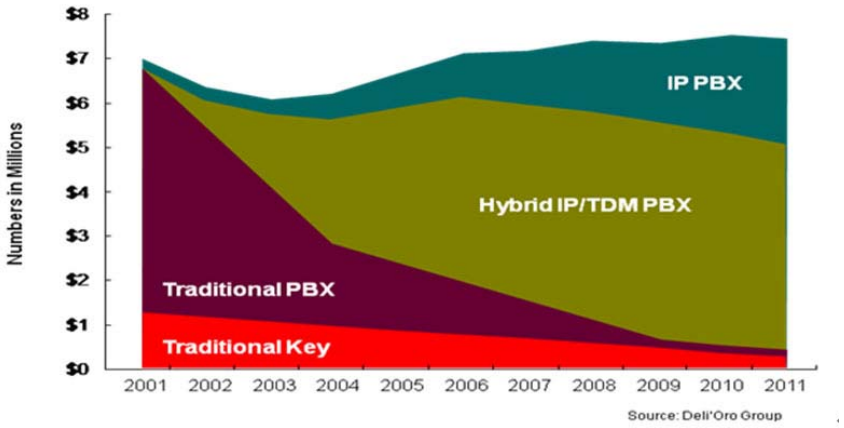
〈그림 10〉 IPT의 Telephony 시장 점유율



출처 : Synergy Research Group

〈그림 11〉은 PBX 기술의 전체의 수익분배를 보여준다. 하드웨어를 기반으로 한 Traditional PBX Key와 Traditional PBX의 수익이 우세했으나, 최근 몇 년 사이 하드웨어에 초점을 둔 Hybrid PBX가 수익이 좋았다. 하지만, 몇 년 후에는 Hybrid PBX의 수익은 더욱더 소프트웨어 구성요소들에 의한 비중이 높아질 것이다. 하지만 Hybrid PBX는 소프트웨어적인 한계 때문에 IP-PBX에 비하여 효율성이 떨어진다. 또한 통신환경이 IP기반 환경으로 변화됨에 따라 점차적으로 IP-PBX 수익률이 높아지고 있다.

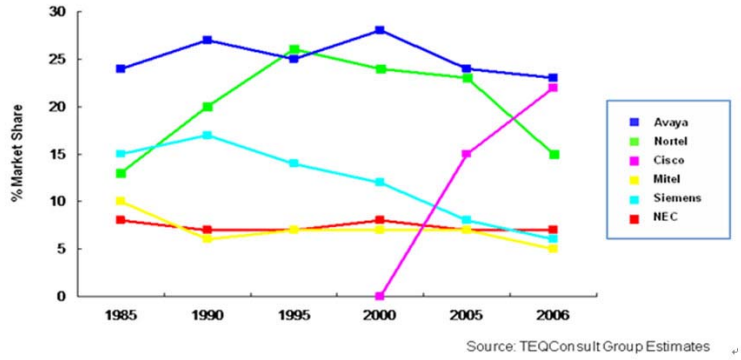
〈그림 11〉 전체 PBX 수익



출처 : Dell'Oro Group

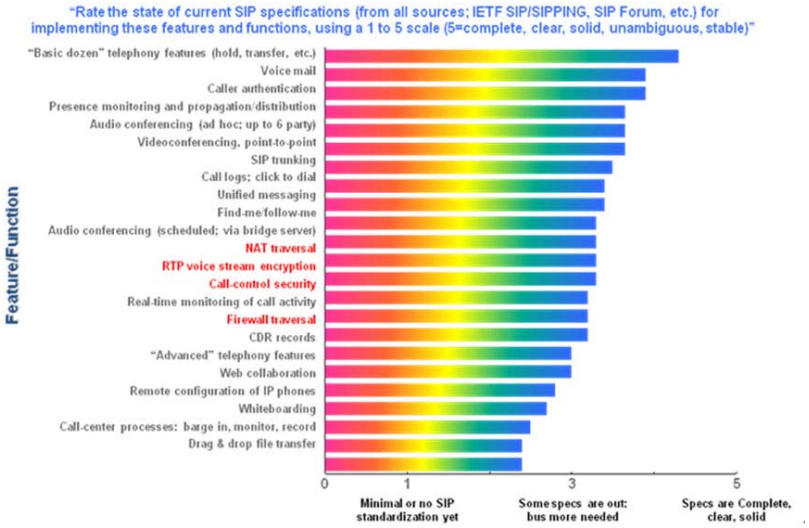
아래의 〈그림 12〉는 PBX 시장 점유율 동향을 나타낸 그림이다. 최근 IP Telephony의 발전은 PBX 시장의 균형경쟁의 두드러진 변화이다. 이러한 변화를 주도하고 있는 Cisco는 최근 몇 년 사이 PBX 시장의 상위로 빠르게 성장하였고, 다른 경쟁 업체들을 압도하고 있다(이 자료는 선적량을 기반한 데이터이다).

〈그림 12〉 PBX 시장 점유율 동향



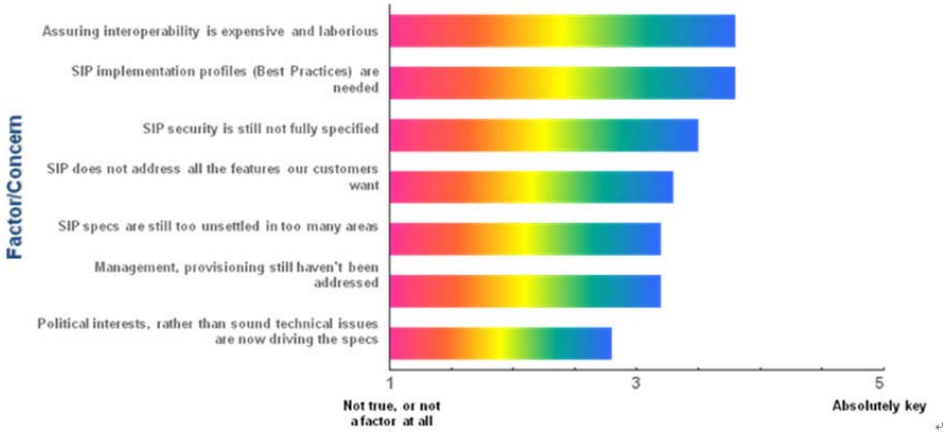
출처 : TEQConsult Group Estimates

〈그림 13〉 SIP Spec 현황(2007)



위의 〈그림 13〉은 SIP Spec 상의 특징 및 기능의 현황을 나타낸 것으로, 전체적으로 볼 때 기본적인 음성 통화 관련된 기능들은 안정화 되어가고 있는 것을 볼 수 있다. 여기서 주목해야 할 것은 "보안및 NAT traversal, Firewall traversal" 기능들로 앞으로 좀 더 성능상 개선이 필요하다. 보안의 경우 세부적으로 RTP 음성스트림, 암호화, Call-Control 보안에 관련된 부분의 안정화가 더 필요하다.

〈그림 14〉 SIP의 직면한 문제



위의 〈그림 14〉은 SIP 전환하는데 있어서 이슈와 직면한 취약점 문제에 대한 것으로, 독립적인 제품간의 상호연동과 보안 문제 해결이 SIP가 성공하는데 있어서 키를 쥐고 있다는 것을 보여주고 있다.

〈그림 15〉 각 IP-PBX 업체별 지원 SIP 기능 비교

Vendor/IP-PBX	SIP Role/Other Protocol Support	Number of SIP Features	Per SIP RFCs	Per SIP Drafts	Proprietary	SIP Security(2)	Third-party SIP Endpoint Support	SIP Trunking	Carrier Interop Via SIP Trunks
3Com/VCX	Native SIP only	175	55%	42%	3%	Authent	12vendors	Yes	1cited
Adtran/ NetVanta	Native SIP, and TDM (T1, PRI)	50	50%	40%	10%	Authent, IPsec VPNs	1vendors	No	-
Alcatel-Lucent/ OmniPCX	Multistack:H.323, Q.sig, others	16	100%	0	0	Authent, IPsec, some encryption	4vendors	Yes	17cities
Avaya:SIP Enablem't Services	Multistack:H.323, Q.sig, others	60	10%	0	90%	Authent, TLS	17vendors	Yes	5cities
BroadSoft/ BroadWorks	Native SIP only	321	100%	0	0	Authent	15vendors	Yes	7cities
Centile/ IntraSwitch	Multistack:MGCP, Cisco prop (SCCP)	85	76%	12%	12%	Authent	10vendors	Yes	1cities
Cisco/ CallManager	Multistack:MGCP, H.323, Cisco prop	176	50%	10%	40%	Authent, TLS, sRTP	None specified	Yes	-
Escaux/ net.PBX	Multistack:H.323, Asterisk prop (IAX)	50	30%	20%	50%	Authent	10vendors	Yes	2cities
Mera Systems	Multistack:H.323	10	100%	0	0	Authent	3vendors		-
Mitle/3300 ICP	Multistack/ Mitel prop (MiNet)	300+	3%	0	97%	Authent	9vendors	Yes	5cities
Nortel:MCS 5100 & CS 1000	Multistack:H.323, Nortel Prop (Unistim)	450+	10%	30%	60%	TLS, sRTP	9vendors	Yes	2cities
pbxnsip/IP-PBX	Native SIP only	30	90%	10%	0	Authent, TLS, sRTP	10vendors	Yes	3cities
Pingtel/ SIPxchange	Native SIP only	174	90%	10%	0	Authent	7vendors	Yes	5cities
Siemens/ HiPath 8000	Multistack:MGCP	100	40%	45%	15%	Authent, TLS	8vendors	Yes	-

IP-PBX 벤더들이 지원하는 SIP 기능을 비교한 내용이다. 표준을 따르고 있지는 여부와, SIP 보안 적용 방식, 서드 파티 단말 지원여부, SIP 트렁킹등 다양한 부분에서 비교 내용을 보여준다. 특히 눈여겨봐야 할 것은 보안 관련된 부분과 서드 파티 단말 지원 부분이다. 단일 IPT장비를 도입할 때는 문제가 되지 않지만, 이기종 단말 및 시스템 도입 시 시스템간 보안 연계 및 서드 파티 단말 지원부분은 꼭 확인할 필요가 있다. 이는 차후 시스템 도입 시 반드시 고려해야 할 사항들이다.

나. 국내 IPT 업체 동향

국내 IPT 관련업체들의 IPT 제품들의 현황을 파악할 필요가 있다. 특히, IPT 관련 기술을 가지고 있는 삼성과 제너의 IPT 제품들을 스펙과 서비스들에 대해 살펴보겠다. 삼성의 경우 Hybrid IP-PBX로 유선 LAN, 무선 LAN, WCDMA등의 접속 미디어를 통합 운영 및 관리 할 수 있는 특징을 가지고 있는 반면 Hybrid IP-PBX는 PSTN망과의 연동은 뛰어나지만, IP기반 서비스에 제약성을 가지고 있다. 제너의 경우 Pure IP-PBX로 VoIP 프로토콜 시그널링만 처리 가능한 All-IP기반의 호처리 장치이다. PSTN과 연동을 위해서는 별도의 게이트웨이가 필요하지만 All-IP 환경에서 제공할 수 있는 서비스

제약이 없다는 강점을 가지고 있다.

〈표 8〉 삼성 IP-PBX 시스템 사양 및 기능

구분		사양	기능
Infra structure	OfficeServ IAP (Call Server)	- IP단말 및 TDM 모듈 최대 50,000회선 수용 - .200,000 BHCA제공	- 구내,외 IP 및 TDM간 Voice 통신 - 모든 단말의 Call Processing 담당
	W-LAN Switch	-802.11x -802.3af 제공 -Subnet간 로밍 제공	WLAN QoS, 보안 등을 담당하는 W-LAN 전용 Switch
System Manage-ment	IP Terminal Manger	-리눅스 OS 사용 (이중화) - Intel 계열 Server 사용	IP 단말의 Call Routing 담당
	QoS Monitor	-Windows XP Professional -Intel 계열 Server	IP 단말의 QoS 관리를 위한 Monitoring Tool
	MAT	-Windows XP Home Edition -Intel 계열 Server	System+Device D/B Config. 프로그램
	Smart iView	-Windows XP Professional -MS SQL Server 8.0 이상	System+Deviec 상태 조회/진단 프로그램
	Comm. Server	-Windows XP Professional (이중화)	Media Gateway, 부가장비간 Data Gateway

〈그림 16〉 Xener IP-PBX 시스템

제너의 IPT 솔류션은 위에서도 언급했듯이 소프트웨어 기반 솔류션이다. IP-PBX는 제품별로 차이가 있지만, 최대 4만 명을 수용할 수 있다.

1. IPv6 기술 및 동향

가. IPv6 도입 배경

현재 사용하고 있는 32비트 IPv4 주소체계는 약 43억 개의 주소 생성이 가능하나 초기의 비효율적인 주소할당과 인터넷의 급격한 발달에 따른 주소 수요의 급증으로 한계점에 근접하고 있다. 특히 유비쿼터스 사회로의 전환에 의해 많은 가전제품과, 이동 통신 단말 등의 IP화가 속도를 더하여 주소 부족 문제를 더욱 심화하고 있다. 이러한 주소 부족 현상의 임시적인 해결을 위하여 CIDR(Classes Inter-Domain Routing), NAT(Network Address Translation), DHCP(Dynamic Host Configuration Protocol) 등의 방식이 고안되어 사용 중이지만 궁극적인 해결책이 되지는 못하기 때문에 새로운 주소체계인 IPv6가 나오게 되었다.

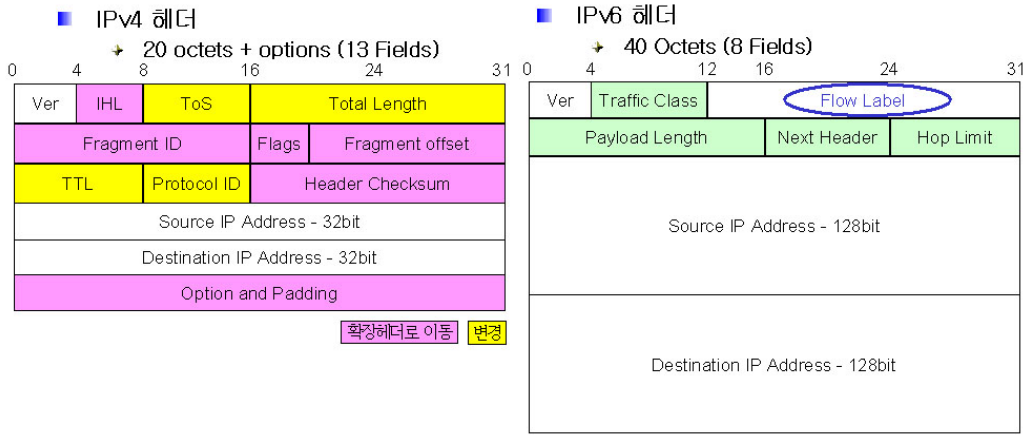
IPv6 주소는 128비트로 3.4×1038개의 주소를 생성하여 주소 부족문제를 해결할 수 있을 뿐 아니라 이동성, 품질제어, 보안, 자동네트워킹 및 다양한 서비스 제공이 용이한 차세대 주소체계이다. 또한 통신·방송 융합, 유무선 통합, BcN, 홈네트워크, 사물의 정보화 등과 같은 유비쿼터스 네트워킹을 지원하기 용이하다.

나. IPv6 주소할당 및 관리

◎ IPv6 헤더 형식

IPv6의 주소형식은 128bit를 사용함으로 IPv4에 비해 두 배 가량 증가하였지만 IPv6 헤더의 필드수를 12개에서 8개로 단순화 시켜 오히려 처리속도를 개선하였다. 〈그림 17〉에서 보듯이, IPv4 헤더의 일부 필드는 같은 기능의 다른 필드로 교체되었고, 잘 사용되지 않는 필드들은 삭제되거나 확장헤더로 옮겨져 필요할 때만 사용되게 하여 기본헤더의 간략화를 통한 헤더처리 효율을 높였다. 그리고 Flow Label이라는 필드를 새로 추가하여 향 후 IP 망의 주요 이슈인 QoS 제공을 위한 기반을 마련하였다.

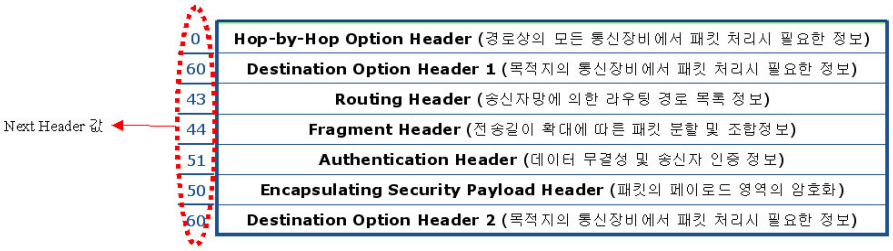
〈그림 17〉 IPv6와 IPv4 기본 헤더 비교



그림에서의 Version 필드(4bit)는 인터넷 프로토콜의 버전을 나타내는 필드이고, Traffic Class 필드(8bit)는 IPv4의 TOS 필드와 같이 트래픽의 등급을 명시해주는 역할을 한다. 다음으로 Flow Label 필드(20bit)는 새롭게 추가된 필드인데 이 필드는 IPv6 패킷이 속하는 Flow에 대한 특성을 나타내는 역할은 한다. 이 필드에 대해서는 아직 표준화 되지 않았지만, Flow 기반의 QoS 관련 그룹의 활동 결과가 추후에 반영될 것이다. Payload length 필드(16bit)는 IPv4 헤더의 Total Length와 같은 기능인 데이터의 길이를 표시하며, Next header 필드(8bit)는 IPv4의 protocol ID 필드와 유사한 기능으로 IPv6 기본헤더 다음 헤더의 종류를 표시하는 기능을 한다. 즉 이 필드의 값에 따라 기본헤더 다음이 확장헤더인지 TCP/UDP 헤더인지를 알 수 있다. 마지막으로 Hop limit 필드는 IPv4의 TTL(Time to Live) 필드와 같은 기능으로 거쳐 갈 수 있는 최대의 라우터 수를 명시한다.

IPv4의 헤더에서 조각화/재조립 등의 자주 사용되지 않는 필드들은 삭제되거나 확장헤더로 옮겨졌다. IPv6의 확장헤더는 이와 같이 잘 이용되지 않았던 필드나 옵션들을 위한 것으로 필요할 때만 사용할 수 있게 하여, 기본헤더를 간략화 시킬 수 있게 하였다. IPv6의 확장헤더의 종류와 기능은 다음 〈그림 18〉과 같다. 확장헤더는 필요한 경우에만 사용되며 기본 헤더의 Next header필드에 해당 값을 표시하여 사용하게 된다.

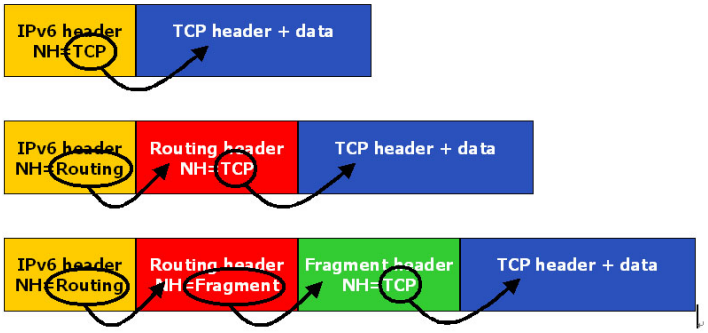
〈그림 18〉 IPv6 확장헤더



옵션헤더는 두 종류가 있는데, 지나가는 홉마다 처리할 옵션을 포함하는 Hop-by-hop Option Header와 IPv6헤더의 목적지 주소에 명시되거나 라우팅 목록에 포함된 노드에서만 처리하는 옵션 정보를 포함하는 Destination Option Header가 있다. Routing Header는 소스 라우팅을 위한 헤더이고, Fragment Header는 조각화/재조립을 위한 정보를 갖는 헤더로서 발신지와 목적지 노드에서만 사용될 수 있다. Authentication Header와 Encapsulating Security Payload Header는 망 계층에서 보안 서비스를 제공하기 위한 헤더이며, 이를 위한 기본 기법 등은 IPSec 그룹에서 표준화를 진행 중이다.

〈그림 19〉은 Next Header 필드를 이용하여 확장헤더를 사용하는 예시를 나타내는 그림이다. 확장헤더가 필요 없는 경우에는 Next Header 필드에 TCP 헤더값(6)을 표시하여 바로 TCP 헤더로 넘어가고, 확장헤더 중에 Routing Header를 사용하고자 할 때는 Next Header 필드에 Routing Header값(43)을 표시하여 사용한다. 각각의 확장헤더에도 Next Header 필드가 있어서 다음 확장헤더 혹은 TCP/UDP 헤더값을 표시하게 된다.

〈그림 19〉 확장헤더의 사용 예시



◎ IPv6 주소 표기 형식

IPv6 주소의 표기는 8개의 16진수 4자리 숫자를 콜론(:)으로 구분하여 표시한다. 즉, 16진수의 한 숫자를 "X"라고 한다면 IPv6 주소는

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

표기 될 수 있다. 그러나 위의 표기 방식이 너무 길고 복잡하기 때문에 중간에 0이 연속되어 있는 구간에 대해서는 한번에 한하여 두 개의 콜론(::)으로 표시할 수 있다.

2002:0000:0000:0000:0000:0000:0000:1001
→ 2002::1001

그리고, IPv6 주소의 총 128bit 중에서 상위 64bit는 주소의 종류와 서브넷을 판별할 때 사용하는 prefix 영역이고, 하위 64bit는 네트워크에 연결되어 있는 각 인터페이스들을 구별하기 위한 interface ID이다. IPv6 주소는 논리적인 계층구조에 따라 이용되기 때문에 상위 노드의 정책에 의해 prefix가 정해진다. 즉, 일반적인 128 bit의 주소 표기만으로는 어디까지가 prefix 영역인지 구별할 수 가 없다. 따라서 prefix에 대한 정보를 "/" 다음에 10진수로 표시해서 prefix의 비트단위를 나타낸다. 예를 들어 prefix 길이가 48bit인 경우에는 네트워크 영역을 나타내는 64bit 중에 48bit가 이미 정해졌다는 의미를 가지며, 즉 나머지 16bit를 이용하여 서브넷 할 수 있다. 이러한 경우에 대한 표기 방법은 아래와 같다.

2001:1000:2000:: /48

◎ IPv6 주소의 종류

IPv6의 주소 종류로는 유니캐스트(unicast), 애니캐스트(anycast), 멀티캐스트(multicast)가 있다. IPv4와 비교 하면 브로드캐스트 주소가 없어졌고 애니캐스트 주소

가 새로 생겨났다. 이들 3가지의 주소에 대한 설명은 다음과 같다.

- 유니캐스트 주소

단일 인터페이스를 지정하며, 유니캐스트 주소로 보내진 패킷은 그 주소에 해당하는 인터페이스에 전달된다.

- 애니캐스트 주소

여러 노드에 속한 인터페이스의 집합을 지정하며, 애니캐스트 주소로 보내진 패킷은 그 주소에 해당하는 인터페이스 중 하나의 인터페이스에 전달된다. 현재는 멀티캐스트 주소에 그 기능이 포함돼 있어서 거의 사용하지 않는다.

- 멀티캐스트 주소

여러 노드에 속한 인터페이스의 집합을 지정하며, 멀티캐스트 주소로 보내진 패킷은 그 주소에 해당하는 모든 인터페이스에 전달된다. IPv6에는 브로드캐스트 주소는 없고, 그 기능은 멀티캐스트 주소로 대체됐다. 현재 어드레스 공간의 15%는 초기 할당됐고, 나머지 85%는 미래를 위해 예약돼 있다.

IPv6에서 유니캐스트 주소를 할당하는 데는 여러 가지의 형태가 있는데 다음 〈그림 20〉가 한 예이다. 예를 들어 2001:2b81:33bb::1234/32의 경우에 상위 32비트 2001:2b81은 subnet prefix가 되고, 하위 96비트인 33bb::1234는 interface ID가 된다. LAN이나 IEEE-802 MAC 주소를 갖는 환경에서의 일반적인 유니캐스트 주소의 구조도 나타낸다. 48비트 interface ID는 IEEE-802 MAC 주소로서 IPv6주소가 설정된다.

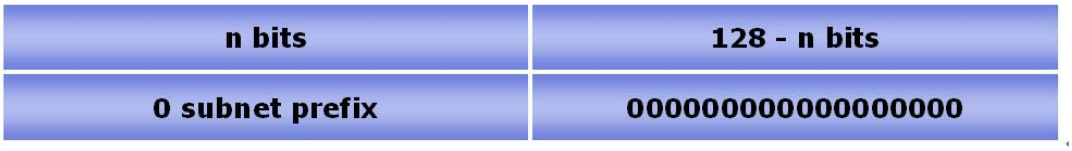
〈그림 20〉 유니캐스트 주소의 예

유니캐스트의 주소형식	n bits	128-n bits	
	Subnet prefix	Interface ID	
MAC주소를 갖는 유니캐스트 주소의 예	n bits	80-n bits	48 bits
	Subscriber prefix	Subnet ID	Interface ID

유니캐스트 주소는 Global, Linklocal, Loopback, unspecified, IPv4 mapped, IPv6 compatible 등으로 구분된다. Global IPv6 주소는 글로벌하게 라우팅 되는 일반적인 주소로서 왼쪽 2개의 비트가 모두 0으로 시작된다. Linklocal 주소는 같은 링크 상에서만 사용되는 주소로 왼쪽이 FE80으로 시작된다. Loopback 주소는 ::1로 표기되고, unspecified 주소는 ::0으로 표기되는데 네트워크 상에서 자기 자신의 주소, 정해지지 않은 모든 주소 등으로 사용된다. IPv4 mapped주소와 IPv6 compatible주소는 IPv4 주소를 IPv6 주소로 표현하는 방법인데 애플리케이션에서는 IPv4 mapped주소, 네트워크 상에서는 IPv6 compatible주소가 터널 주소로 활용된다.

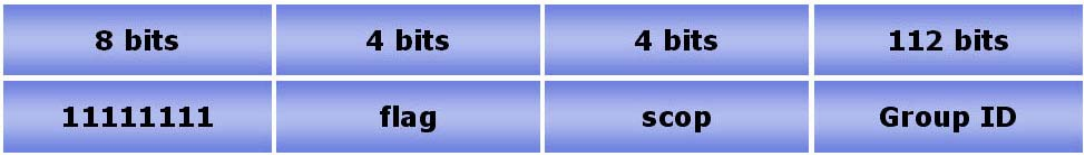
애니캐스트 주소는 라우팅 프로토콜의 거리 측정을 통해 같은 애니캐스트 주소를 갖는 인터페이스 중에서 가장 짧은 거리에 있는 인터페이스에 전달된다. 애니캐스트 주소는 유니캐스트 주소 공간으로부터 할당 되어 유니캐스트 주소의 구조를 갖기 때문에 구문적으로 유니캐스트 주소와 구별할 수 없다. 애니캐스트 주소는 IPv6 패킷의 소스 주소로 사용될 수 없고, IPv6 호스트에 할당 될 수 없으며 단지 IPv6 라우터에만 할당될 수 있는 주소이다. IPv6의 애니캐스트 주소는 IPv4 상에서의 DNS의 미러서버에서 로드발런싱 등의 용도로 사용됐던 주소와 비슷한 개념이라 할 수 있다. 애니캐스트 주소의 구조는 다음 〈그림 21〉와 같다.

〈그림 21〉 애니캐스트 주소 구조



멀티캐스트 주소는 상위 8bit가 FF(11111111)값을 가짐으로써 유니캐스트 주소와 구별된다. 멀티 캐스트 주소의 구조는 다음 〈그림 22〉과 같다.

〈그림 22〉 멀티캐스트 주소 구조



멀티캐스트 주소의 종류에는 여러 가지가 있는데 자주 사용되는 주소를 나열하면 다음 〈표 9〉와 같다.

〈표 9〉 멀티캐스트 주소의 종류

Address	Meaning	Scope
FF01::1	모든 노드	Node-local(loopback)
FF02::1	모든 노드	Link-local
FF01::2	모든 라우터	Node-local
FF02::2	모든 라우터	Link-local
FF05::2	모든 라우터	Site-local
FF02::1:FFXX:XXXX	Solicited 노드	Link-local

다. IPv4 대비 IPv6의 장점

IPv6의 특징으로는 IP 주소의 크기가 32비트에서 128비트로 증가됨으로써 주소 공간이 확장되었을 뿐만 아니라 주소 범주의 정의, 생존시간 설정, 주소 자동 설정 및 애니캐스트 지원 등 그 활용 범위도 대폭 증대 되었다. 그리고 헤더의 크기가 커졌음에도 불구하고 간략화 및 고정화된 기본헤더 형식의 사용으로 처리 속도는 더욱 개선되었다. 그 외에도 인증, 데이터 무결성, 데이터 기밀유지 등을 위한 확장 헤더가 정의 되어 보안 서비스 제공이 용이하다.

IPv6는 IPv4와 비교했을 때 기본 구조와 헤더구조의 변화만으로도 다음과 같은 많은 장점을 지원한다.

◎ **주소공간의 확대**

- 주소 개수의 증가
- 주소구조 계층의 레벨 수 증가로 인한 새로운 주소 정의 가능
  - 멀티캐스트 주소뿐만 아닌 애니캐스트 주소 가능

◎ QoS 지원

- 기본헤더 2번째 필드(Traffic Class)에서 등급별 우선순위 지급
- 기본헤더 3번째 필드(Flow Label)에서 QoS를 위한 서비스별 구분 표시

◎ IP 자체의 보안성 확대

- IPSec가 프로토콜 내에 탑재
- 인증, 데이터무결성, 데이터 기밀유지 지원을 위한 확장헤더 정의

◎ **헤더 형식의 단순화**

- 옵션 필드를 확장헤더로 옮김
- 오버헤더의 최소화/단순화
- 전체 필드 수를 8개로 단순화시킴으로 인한 처리속도의 개선

◎ **이동성 지원 (Mobile IPv4 대비 장점)**

- 최초 설계단계에서 MIPv4의 시행착오를 반영하였으므로 효과적인 이동성 지원
- 경로 재설정 기본 지원
- CoA 주소의 사용으로 Ingress Filtering 문제 해결
- Foreign Agent 필요 없음(CoA 주소 자동 생성)
- 기본적으로 보안지원(IPSec)

다음 〈표 10〉는 IPv4와 IPv6를 비교하고 IPv6의 장점을 정리한 것이다.

〈표 10〉 IPv4와 IPv6 비교표

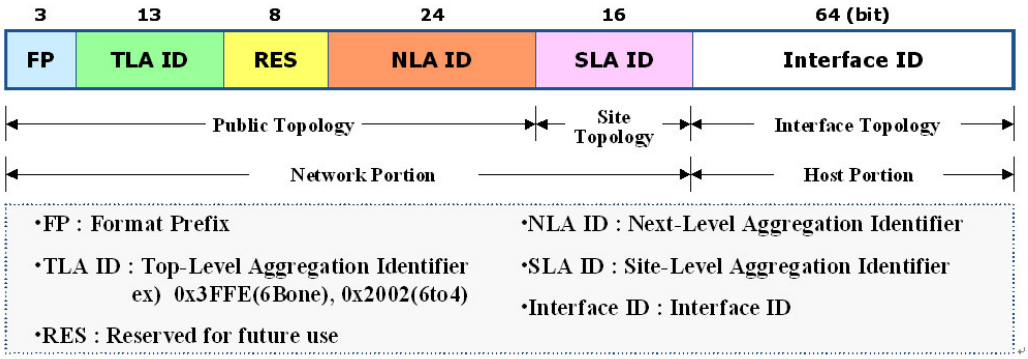
구분	IPv4	IPv6	IPv6 장점
주소공간	2개 (약 43억 개)	2개로 거의 무한대	경찰통신망의 ALL IP화 대비 가능 사설주소의 제거로 P2P 통신환경 조성 가능
주소할당	초기 체계적이지 않은 비효율적 할당으로 주소낭비 초래	IPv4의 경험을 교훈 삼아 초기부터 체계적이고 효율적인 주소 할당을 꾀하고 있음	체계적인 주소할당에 이어 각 사이트에서는 계층화 구조를 갖는 네트워크 설계 가능
사용편이성	수동설정, DHCP	Stateless Address 자동설정	Mobility 분야 등 적용
Mobile IP	문제점 많음	최초 설계단계에서부터 반영 (DestinationOptionHeader)	향후 정보통신망의 핵심 트랜드인 Mobile, QoS, 보안 서비스 수용 용이
QoS 지원	QoS 필드 제한적	Flow Label 추가	
보안기능	IPSec 별도	IPSec 내장 (AuthenticationHeader,EncapsulatingSecurityPayload Header)	
자동 네트워킹	곤란 (Manual Configuration)	가능 (Auto Configuration)	네트워크 관리 용이
헤더옵션 처리	헤더 옵션이 포함된 상태	필드수의 간략화(8개) 및 고정화	헤더처리 속도 향상

라. IPv6 주소의 할당

IPv6 핵심 프로토콜의 표준화 작업과 함께 IPv6 주소할당에 대한 이슈는 IPv6의 실용화와 관련된 가장 중요한 이슈라고 할 수 있다. IPv6 주소는 128bit로 표현되는데 RFC에 의거한 기술적 경계인 64bit를 기준으로 상위 64비트는 네트워크 주소로서 라우팅과 연계된 네트워크 구분자로 활용되고, 하위 64비트는 인터페이스 주소로서 하나의

서브넷 망에서의 LAN카드 및 Chip 등의 단말의 구분자로 활용된다. 그리고 기술적 경계 앞부분의 64bit를 RIR(Regional Internet Registry)내 협의에 기초한 정책적 경계인 48비트와 16비트로 나누어서 앞의 48비트는 상위 네트워크 주소로 활용하고 뒤에 16비트는 하위 네트워크 주소로 활용한다. 다음 〈그림 23〉은 IPv6 주소의 할당 구조를 나타낸 것이다.

〈그림 23〉 IPv6 주소의 할당 구조



IPv6 주소는 인터넷의 장기적 관점에서 신중하게 관리되어야 하는 공공재이다. 따라서 유일성, 등록성, 집합성, 보존성, 공평성, 간편성, 목적지간 충돌방지 등의 목적을 갖고 관리되고 있다. 전 세계의 IP주소 및 AS번호는 IANA(Internet Assigned Numbers Authority)에서 총괄 관리된다. IANA의 위임 하에 대륙 단위로 해당 영역의 주소를 관리하는 대륙 별 인터넷주소관리기관으로 RIR(Regional Internet Registry)가 있으며 아태지역의 APNIC, 북미지역의 ARIN 등이 있다. 그리고 해당 영역의 RIR의 위임에 따라 해당국가의 인터넷 주소를 관리하는 국가별 인터넷 주소관리 기관으로는 NIP(National Internet Registry)가 있으며 대한민국의 KRNIC, 일본의 JPNIC 등이 그 예이다. 인터넷 공동체는 RFC 1881을 통해 IANA를 전 세계 IPv6 주소관리의 책임을 가지는 기관으로 합의를 하였고, 이후 IANA는 하위 규모의 IPv6 주소에 대한 분배 역할을 RIR에 위임하였다.

IANA의 RIR에 대한 초기 주소분배는 RFC2928에 의해 정해졌는데, 전체주소 중 앞

의 3비트 주소가 '001'인 Global 유니캐스트 주소를 기준으로 16비트까지의 주소를 활용하게 된다. 즉, 한 개의 /16을 128개의 /23으로 나누고, RIR의 요청에 따라 한 개의 /23씩을 대륙별로 분배하게 된다. IANA로부터 /23 단위로 주소를 확보한 RIR은 64개의 /29를 구성하여 활용하는데, NIR이나 ISP의 주소 요청이 있으면 최초의 /29(8개의 /32) 중에 1개의 /32를 배분하고 나머지는 향후의 사용을 위하여 해당 NIR이나 ISP를 위해 예약된다. IPv6 주소 초기 배정 신청 기관의 요건으로는 LIR(ISP 포함)이어야 하고 최종 사용자가 아니어야 한다. 그리고 /48이상을 할당할 기관들에게 IPv6 접속서비스 제공 계획을 가지고 있어야 하고 해당 IPv6 주소를 라우팅 해야 하며 2년 내에 200개 이상의 가입자(기관) 확보 계획을 가져야 한다. 기본적인 초기배정의 규모는 /32이나 주소 신청 요건 및 관련 자료에 따라 변경이 가능하다. IPv6 주소의 추가 배정 신청을 위한 기관의 요건은 기 배정된 IPv6 주소를 보유하고 있어야 하고 기 배정된 IPv6 주소의 사용 밀집도(HD ratio)가 한계값(0.8) 이상인 경우이어야 한다. 즉, 초기 /32 1개를 배정받은 경우라면, 최소 7,132개의 /48 이상을 할당해야 IPv6 주소의 추가 배정을 받을 수 있는 것이다. 추가 배정 시에는 초기 배정 규모의 2배를 배정받을 수 있으며(초기에 /32 1개를 배정받은 경우, 31/ 1개를 배정 받음) 초기 배정의 2배 이상의 추가 배정 신청 시에는 이에 상응하는 관련 자료를 추가적으로 제출하여야 한다.

end-site에게 IP 주소 블록을 할당하는 정책은 RIR에서 정하고 있으나 IAB/AESG 등에서 기술적인 사항을 고려하여 권고안을 제공하고 있다. IETF와 RIR의 전문가 들이 모여 2001년 9월에 함께 정의한 RFC3177에 따르면 /48이 공중망과 사설망의 경계를 정의하는 하나의 최종사업자(end-site)에 할당되는 충분한 주소라고 정의 하였다. end-site의 주소할당은 다음과 같다.

◎ /128 할당

하나의 장비가 연결되는 경우로 오직 하나의 디바이스만 연결되는 가입자

◎ /64 할당

하나의 서브넷이 필요한 경우로 오직 하나의 서브넷을 갖는 가입자

◎ /48 할당

가장 일반적인 홈네트워크 및 SOHO, 그리고 65,536개 이하의 서브넷을 갖는 기업의 가입자, ADSL 또는 CATV 가입자, 단일 컴퓨터를 가진 가입자가 홈네트워크 등으로 향후 서비스 확장이 예상되는 경우

◎ /48 이상 할당

하나의 최종사용자가 초기 /48 이상 또는 추가적인 /48 주소 배정을 요청할 경우에 Second Opinion Request를 신청

2. 국내 IPv6 도입 및 사례 분석

경찰통신망의 IPv6 이행 모델 수립에 앞서 주요 공공기관들의 사례들을 분석하여 시사점을 도출하고, 이를 토대로 경찰통신망 IPv6로의 이행 모델을 수립하는데 참고하고자 한다.

국내의 사례로는 KOREAv6의 시범서비스, 정보통신부와 한국전산원의 '공공기관을 위한 IPv6 도입 전략 수립', '부산시청 IPv6 이행환경 분석 및 도입방안 수립'등을 살펴보고 경찰통신망의 IPv6 이행모델 수립 시 참조할 수 있는 시사점을 도출하겠다.

한국전산원에서 2004년 7월부터 IPv6 시험망을 확대 구축하고 IPv6 시범서비스 및 IPv6 장비 그리고 솔루션의 시험운영을 수행하는 KOREAv6 시범사업을 추진하여 각 분야별로 적합한 IPv6 서비스 모델을 검증하였다. 시범사업에서는 ISP분야, 이동 통신 분야 등 9개 분야에 대한 IPv6 이행 모델을 마련하였는데, 그 중에 ISP분야(통신사업자의 IPv6 인터넷서비스), 학교분야(학교 내에 IPv6 시스템/ 응용서비스 도입 및 이용활성화), 기업분야(기업내 VoIPv6 시범서비스)의 이행모델에 대하여 살펴본다.

◎ 단계별 서비스 구성

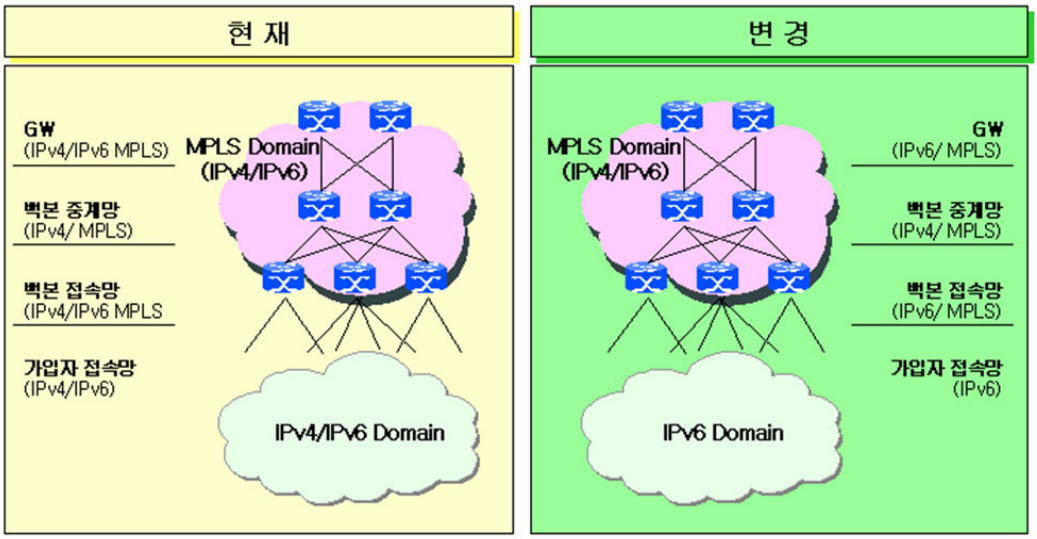
1단계 는 IPv6 이행을 위한 사전준비 단계로 백본에 MPLS만 탑재하였으므로 기존서비스와의 차이점은 없으며, 다만 MPLS를 이용한 IPv4 기반의 부가서비스를 창출할 수 있다.

2단계에서는 6PE간에만 통신이 가능하므로 중대형 기관 및 기업을 대상으로 IPv6 서비스를 실시할 수 있으며 컨텐츠의 집합소인 IDC 센터에 IPv6 서버팜을 수용할 수 있다. 또한 최종 가입자 접속노드에는 IPv6가 올라가지 않아 일반 가입자에게는 Native IPv6 서비스를 제공할 수 없으며 다양한 터널기법을 적용하여 IPv6 연결서비스가 되도록 구성하여야 한다.

3단계에는 모든 망 구간에 IPv6가 탑재되어 일반 가입자에게도 Native IPv6 서비스를 제공할 수 있으나 아직 IPv4와 IPv6가 공존하는 단계이므로 다양한 변환기술을 이용하여 IPv4와 IPv6간의 통신이 가능하도록 구성하여야 한다.

4단계에서는 모든 네트워크가 듀얼스택으로 구성된 상태에서 자연스럽게 IPv4를 제거하여 Only IPv6로 진화하는 최종단계이며 IPv6만의 새로운 서비스가 가능하다.

〈그림 24〉 4단계 진화 모델



◎ 핵심성공요소 (KSF)

- 기존 IPv4망과의 연동

새로 개발한 응용서비스를 다양한 고객 환경에 맞춰 제공하기 위해서 기존 IPv4망과의 연동이 반드시 필요하다. 대부분의 가입자와 기관들이 IPv4망에 연결되어 있고 다양한 시스템과 장비 및 네트워크 자원들 대부분이 IPv4로 되었기 때문이다.

- 이용자 확보를 위한 서비스 개발

인터넷 보안서비스(VPN 포함)와 업무 효율화에 도움이 되는 그룹웨어 서비스, 멀티미디어서비스(채팅, 파일전송, VoIP, 스트리밍 서비스 등), VoD, P2P 등의 IPv6용 응용서비스들이 개발되어야 한다.

- 이용자 확보를 위한 홍보

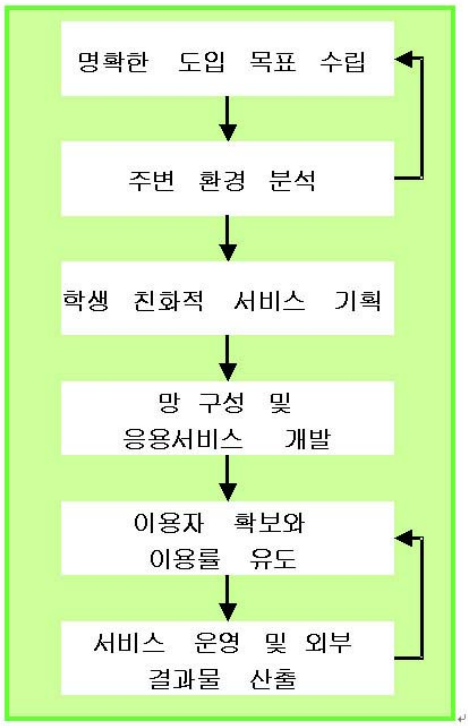
IPv6의 홍보 및 활성화 유도, IPv6 관련 사이트 연계 등의 기능을 가지는 홈페이지 구축과 IPv6 시범서비스를 체험할 수 있는 전시관 구축이 필요하며, 초고속 인터넷 가입자를 대상으로 한 이메일 홍보 역시 중요하다.

◎ 학교 내 IPv6 시스템/응용서비스 이행모델

학교내에 IPv6 시스템/응용서비스 도입 및 이용 활성화를 위해 학내 캠퍼스 네트워크에 IPv6를 도입하고 학생들에게 IPv6 기반서비스를 제공하기 위한 이행모델을 수립하였다. 특히 학교 분야의 이행모델은 일반 상용 서비스가 아닌 수동적 서비스 이용이 주가 되는 학교기관이란 특이성을 고려하여 IPv6망을 구성하였다.

학내 IPv6 서비스 도입절차를 살펴보면, 우선 발생 가능한 여러 가지 문제점들을 사전 예측하여 해결방안을 마련한 뒤 명확한 도입목표를 수립 한다. 목표가 수립되면 교내 망 환경을 비롯한 주변 환경을 조사하여 분석하고, 분석이 끝나면 학생 친화적인 서비스를 기획한다. 즉, 이용자 중심의 이용자 친화적인 서비스를 기획하는 것이다. 서비스 기획이 끝나면 본격적인 망 구성과 응용 서비스 개발을 수행하고 이와 함께 이용자 확보 및 이용률 유도를 위한 홍보 활동을 병행한다. 다음 〈그림 25〉는 위의 IPv6 서비스 도입절차를 나타내는 그림이다.

〈그림 25〉 학내 IPv6 서비스 도입 절차



◎ 핵심성공요소 (KSF)

- 학교 당국과의 긴밀한 협조

교내통신센터와 망 구성 및 운용에 있어서 학교 당국과의 긴밀한 협조가 필요하다. 기존의 IPv4 기반 네트워크를 수정하게 되면 관리적인 측면에서 큰 부담이 따르기 때문이다. 즉, 사전에 망 구성을 충분히 조사하고 통신센터의 입장을 낱낱이 고려한 뒤, 새로운 IPv6 망 구성 계획을 제시하여야 하며, 망 구성에 따른 기대효과를 학교 당국에 충분히 어필하여야 한다.

- 학생들이 쉽게 접근할 수 있는 망 구성

학생들이 자주 이용하는 실습실을 이용하여 시범서비스를 실시함으로써, 서비스를 홍보하고 보다 많은 학생들이 시범서비스에 쉽게 접근할 수 있도록 유도한다. 이를 위해서는

학생들이 이용하기 쉽고 친숙한 서비스의 제공이 필요하다.

- 학생들에게 흥미를 유발 할 수 있는 서비스 발굴

학생들은 호기심이 많고 시간적 여유가 많은 집단으로 관심분야가 비교적 흥미 위주로 나타난다. 따라서 최근 관심을 끌고 있는 휴대 인터넷 환경을 구성하고 비교적 고가인 단말기를 대여하여 서비스 이용을 시킨다면 훨씬 높은 흥미를 유발 시킬 수 있다. 또한 수강신청이나 성적확인 등의 반 강제적인 성격이 강한 서비스를 시범 서비스로 대체함으로써 학생들의 이용을 유발 시킬 수 있다.

- 지속적인 피드백을 통한 서비스 개발

지속적인 설문조사나 다른 의견수렴의 절차를 거쳐 서비스의 신뢰도를 증진 시켜야 한다. 또한 이용자들이 원하는 서비스 정보를 얻고 그에 맞춰 서비스를 개발하여 제공한다면 IPv6 저변 확대에 크게 이바지 할 수 있다.

◎ 기업내 VoIPv6 시범서비스

기존의 PSTN 전화망을 대체할 핵심 기술인 VoIP는 기존의 전화망 사용 할 때보다 비용이 절감되고, 영상회의 등의 부가 서비스 제공이 용이하다. 특히 주소 공간이 풍부하고 이동성이 지원되는 VoIPv6는 많은 장점 들을 갖고 있다. VoIP는 사내 PBX로 구성된 사내전화망을 대체하는 것과 KT, 데이콤 등에서 운영하는 PSTN 전화 사업자망을 대체하는 것으로 나눌 수 있지만, 여기서는 사내 전화망을 IPv6 기반 VoIP로 전환하는 기업 모델에 대해서 설명한다.

기업용 VoIP 시스템 구축 방법은 여러 가지가 있을 수 있는데 대표적인 방법은 다음의 두 가지로 나누어 볼 수 있다. 첫 번째 방법은 자체적인 Gateway가 있어 사내 전화 및 IP 망으로 연결된 다른 기관과의 call은 VoIP로 하고 외부 call은 PSTN으로 자기 회사에 돌려주는 방법이다. 두 번째 방법은 인터넷전화사업자를 통하여 VoIP 통화 및 PSTN 통화를 해결하는 방법이다. 인터넷 전화 사업자는 PSTN으로 연결되는 Gateway를 보유하고 있고 콜 시그널링을 처리하는 서버를 보유하게 된다. 그리고 가입 기관이 PSTN을 사용할 경우 과금하는 형식으로 서비스를 운영한다. 이는 비교적 규모가 작은 회사에서

주로 사용하는 방법이다

VoIP 구축 방법에 대한 결정이 나면 IPv6 네트워크를 구축한다. VoIP 시스템을 위해서는 기업 인트라넷 망뿐만 아니라 외부 익스트라넷 또한 IPv6로 변환해야 한다. 초기 IPv4 애플리케이션 사용을 위한 IPv4/IPv6 Dual 망을 구성하고, IPv4 망과의 연동을 위한 변환기도 구현한다. IPv6 네트워크가 구축 되면, VoIP 시스템 장비를 도입하여 설치하고 최종적으로 VoIP 단말기를 선택하여 설치한다.

3. 공공기관을 위한 IPv6 도입 전략 수립

전자통신부와 한국전산원에서는 공공기관의 성공적인 IPv6 도입 및 전환을 위해 '공공기관을 위한 IPv6도입 전략 수립 지침'을 제시하였다. 지침은 IPv6를 도입하기 위한 방안과 전략을 제시하고 IPv6 전환을 위한 점검 체계 및 방법론을 제시하고 있는데 IPv6 이행모델 수립에 대한 사례도 소개하고 있다. 특성이 다른 두 공공기관(A, B 로 구분)의 이행모델을 살펴보면 다음과 같다.

가. A 공공기관

A 공공기관의 경우, 단계별로 IPv6를 전환함에 있어서 기관 특성에 맞는 영역별 우선 전환 순위를 적용하여 단계적인 IPv6 전환을 추진한다. 첫 번째 단계는 네트워크 부문에 대한 전환으로 각 네트워크 장비(라우터, 스위치, 방화벽 등)의 IPv6 지원 여부를 점검하고 장비의 교체 및 증설 여부를 판정하는 단계이다. 두 번째 단계는 서버 부문에 대한 전환으로 각 서버의 OS 현황을 조사하여 OS의 교체 및 업그레이드를 판정하는 단계이고, 마지막 단계는 응용서비스 부문의 전환으로 응용서비스의 교체 및 업그레이드, 개발 여부를 판단하고 최종적으로 IPv6의 발전전략 및 활용전략을 수립하는 단계이다. 각 단계별 우선 고려 분야는 다음 〈표 11〉과 같다.

〈표 11〉 A 공공 기관 단계별 로드맵

영역	1단계 네트워크	2단계 서버	3단계 응용서비스
우선 분야	○ IPv6 지원여부 점검 ○ IPv6 표준 기술을 지원하는 IPv6 지원 장비 확보 ○ 장비의 교체 및 증설 여부 판정 ○ 라우터 IPv6 전환 ○ 스위치 IPv6 전환 ○ IPv6 지원 방화벽 도입 및 업그레이드 ○ 방화벽 IPv6 전환	○ 1단계에서 진행한 각 네트워크 자원의 IPv6 전환완료 점검 ○ IPv6 OS 교체 및 업그레이드 판정 ○ 서버 시스템 교체 및 증설 여부 판정 IPv6 OS 전환 ○ 응용 서비스 IPv6 전환 준비	○ 2단계의 IPv6 OS 전환 점검 ○ IPv6 지원 응용 서비스 확보 ○ 응용서비스의 교체 및 업그레이드 판정 ○ 응용서비스 개발 여부 판정 ○ 응용서비스 IPv6 전환 ○ 최종 IPv6 전환 점검 ○ IPv6 발전 전략 및 활용 전략 수립

제 1단계에서 네트워크 장비의 IPv6 전환 시 고려할 사항은 업그레이드 가능 장비와 불가능 장비로 구분하여, 가능 장비는 IPv6 지원 모듈 추가 및 OS 업그레이드를 통해 IPv6로 전환하고, 불가능한 장비는 IPv6 전환이 가능한 장비로 교체해야 한다는 것이다. 이때 비용 측면을 고려하여 적합한 장비 및 제조사를 선택하여 교체 하여야 한다. Layer 2 장비의 경우에는 IPv6와 직접적인 관계가 없으므로 기존의 장비를 그대로 사용한다. 네트워크 장비의 IPv6 전환을 마친 후에는 서버 장비와 응용서비스의 IPv6 전환을 수행한다. A 공공기관의 경우 모든 응용서비스에 대한 전환이 어려우므로 주요 응용서비스에 대한 전환만을 고려하였다. 주요 응용 서비스는 메일, 웹, DNS 등이다.

나. B 공공기관

B 공공 기관의 경우에는 해당 기관의 네트워크 구성이 간단하여 단계적인 IPv6 전환으로 구성하지 않고 바로 최종 구성 단계로 모델을 수립하였다. B 기관 역시 주요 응용서비스를 제외한 응용 서비스들은 IPv6 전환에서 제외하고 이행 모델을 수립하였다. B 기관은 네트워크 및 시스템 구성이 복잡하지 않아 IPv6 전환에 큰 어려움은 없었으나 인터넷 연동 라우터를 제외한 대부분의 네트워크 장비, 서버 시스템, 최종 단말, 응용 서비

스들이 IPv6로 전환하기 부적합한 상태였다. 이러한 상황에 맞는 IPv6 전환 이행 모델은 다음과 같다.

라우터 장비는 IPv6 전환이 가능한 백본 라우터를 사용하고 있으며, IPv6를 지원하는 버전의 네트워크 OS를 사용하고 있으므로 IPv6 전환 시 어려움이 없다. 그러나 내부 백본 스위치와 연결되는 L3 스위치가 IPv6를 지원하지 않는 모델일 뿐만 아니라 해당 벤더에 IPv6를 지원하는 장비가 없어 새로운 벤더의 L3 스위치를 도입하는 것이 요구된다. 서버 시스템과 단말 시스템도 IPv6 전환이 가능한 OS로의 업그레이드가 요구된다. 즉, 서버 OS의 경우에는 Windows 2003 Server와 Solaris 2.8 이후 버전으로 업그레이드를 해야 하고, 단말 OS의 경우에는 Windows XP 환경으로의 업그레이드가 필요하다. 이때 업그레이드할 OS를 지원하지 못하는 서버나 단말 사양에 대해서는 새로 교체 하는 것이 바람직하다. 주요 응용 서비스 인 웹, 메일, DNS를 중심으로 IPv6 전환을 수행하고 나머지 응용 서비스는 이후 개발이나 IPv6 지원이 가능한 응용 서비스로의 대체하여야 한다. 방화벽의 경우에도 IPv6 전환이 지원되는 모델인지에 대한 여부 확인이 필요하다.

다. 부산시청 IPv6 이행모델

부산시는 부산 시청의 IPv6 이행 환경과 역량을 파악하고 이에 대한 다각적인 분석을 통하여 지자체 환경에 부합하는 IPv6 이행 모델을 수립하고 정보화 추진 계획 및 지역 발전 정책 등과 연계하여 시너지를 낼 수 있는 IPv6 응용 서비스를 발굴하고, 시범 서비스 추진을 위한 가이드를 도출하기 위하여 '부산시청 IPv6 도입방안 및 비용산정' 과제를 수행하였다. 이를 위하여 사전에 충분한 현황 분석을 통해 이행 로드맵을 정하고, 분석된 고려 사항을 반영하여 단계별 모델을 수립하였다. 이행 모델의 논리적 단계는 준비단계, 진입단계, 본격이행단계, 통합단계로 나누어지고 내용은 다음과 같다.

1) 준비단계(2005~2007)

부산시는 정보고속도로가 구축 되고 원활히 운영되기 위한 사전 준비를 하는 3년동안의 준비단계를 두었다. 준비 단계에서는 타당성 검토, 자원의 교체/ 증설/ 폐기 계획, IPv6 네트워크 구성 모델을 수립하게 된다.

2) 진입단계(2008～2009)

진입단계는 안전한 IPv6 이행 및 위험요소, 기존망과의 호환성문제를 피하기 위해 부산시청 내에 듀얼스택을 구성하여 시범 운영하는 단계이다. 진입단계에는 IPv4/IPv6 듀얼스택 도입에 앞서 듀얼스택 도입과 이행을 위한 가이드라인과 지침을 마련하고 이행한다. 우선 청내의 PC, 서버, 네트워크 장비, 백본 등의 전산자원에 대한 듀얼스택을 적용하고, 6GIX, 6KANet 등과 연동하여 안정성 테스트를 한다. 이후 시청내의 서버, PC 등의 OS 업그레이드를 실시하고 IPv4/IPv6 주소를 동시에 할당 받는다. 신규 도입되는 L3 스위치는 듀얼스택을 지원하는 장비로 구성하여 구청/ 동사무소 등의 IPv4 트래픽을 시청에서 수용할 수 있도록 설계한다. 진입단계에서의 부산시청 인트라넷은 듀얼스택 망으로 운용되며 구청 및 각 동사무소 등은 IPv4망으로 운용된다.

3) 본격 이행단계(2010)

진입단계 이후에는 구청/ 동사무소, 사업소 단위까지 듀얼스택을 확대 적용하는 본격 이행단계로 진행한다. 단 이때는 각 기관별로 전산자원에 듀얼스택만 탑재한 채 시청과 구청/동사무소간 통신은 그대로 IPv4를 이용한다. 백본과 가입자단을 동시에 실시하되 각 구청별 네트워크 자원의 버전업 계획이나 장비 교체주기 상황에 의거하여 우선순위를 정하여 실시한다. 필요 시 단기간에 걸쳐 전체에 대한 업그레이드 실시가 요구될 수 있으므로 본격이행단계 이전에 대비할 필요가 있다.

4) 통합단계(2011～)

마지막으로 듀얼스택 자원에 대해 IPv4 프로토콜 스택을 제거하여 백본망이 IPv4/IPv6 듀얼스택으로 전환되는 시점이 통합 단계이다. 이때 안정적인 IPv4 제거를 위해서는 사전에 이행 지침 수립 및 검증이 반드시 필요하다. 통합단계는 실질적인 부산시 정보고속도로 네트워크의 ALL-IP 로 이행하는 단계로서 이 후의 신규 도입 자원은 IPv6-ONLY를 의무화 하고 Native-IPv6 장비의 도입을 추진한다.

〈표 12〉 단계별 IPv6 네크워크 모델

	시산하 직속기관	부산광역시청	백본망 (10G백본링)	16개 구/군청
진입단계	IPv4 네트워크	v4/v6 듀얼스택	터널생성	IPv4 네트워크
	IPv4	IPv6	IPv4	IPv4
이행단계	v4/v6 듀얼스택	v4/v6 듀얼스택	터널생성	v4/v6 듀얼스택
	IPv4	IPv6	IPv4	IPv4
통합단계	듀얼스택 제거	듀얼스택 제거	v4/v6 듀얼스택	듀얼스택 제거
	IPv6	IPv6	IPv6	IPv6

라. 국내 사례의 시사점

위에서 성격이 다른 몇 가지의 IPv6 전환 이행 모델들을 살펴보았다. ISP분야, 학교분야, 기업 VoIPv6, 공공기관, 부산시청 등의 사례들에서 다음과 같은 시사점들을 도출할 수 있다.

첫째, IPv6 전환 이행 모델을 수립하기 위해서는 사전에 충분하고 정확한 현황 분석이 필요하다. 해당 기관의 네트워크 규모, 네트워크 장비의 제조사 및 버전, 응용 애플리케이션의 IPv6 지원 여부 등에 따라 이행 모델이 크게 달라질 수 있기 때문이다. 즉 확실한 현황 파악이 이행 모델 수립은 물론이고 IPv6 전환에 있어 가장 중요한 작업이라 할 수 있다.

둘째, 이용자 중심의 서비스를 우선 개발하고 보급해야 한다. IPv6 전환 초기에는 이용자들이 새로운 네트워크에 대한 막연한 불안감으로 이용을 꺼릴 수 있다. 따라서 실제 이용자들의 접근이 용이한 망을 구성하고, 이용자에게 친숙한 서비스를 제공하여 보다 많은 이용자가 이용하도록 해야 한다. 이는 IPv6 네트워크의 활성화에 기여하는 것은 물론이고 이용자들의 피드백을 통한 신뢰성 있고 활용 가치가 높은 망 구축에도 많은 도움을 줄 것이다.

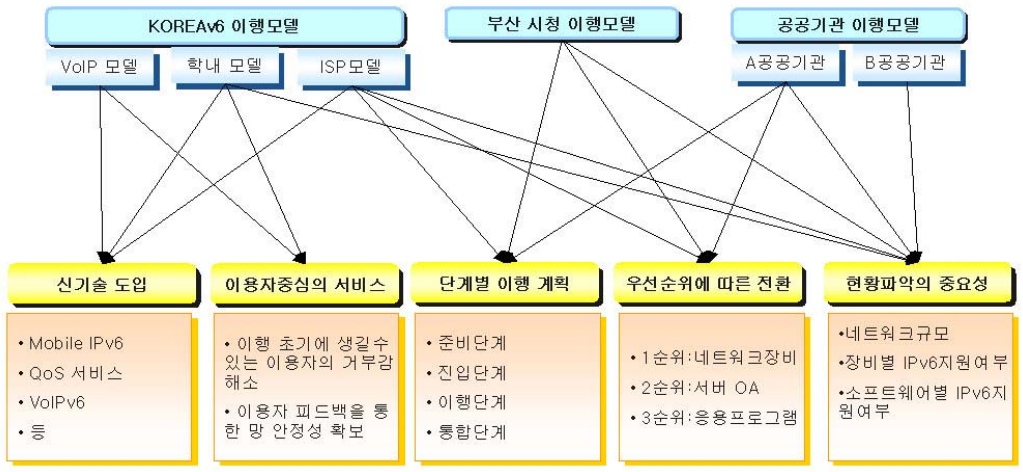
셋째, 단계별 이행 모델을 수립해야 한다. 해당 기관의 규모나 현황에 따라 달라 질 수

는 있지만 보통의 전환 전략은 4단계로 나뉘어 수립된다. 전환 초기의 IPv4와 IPv6가 공존하는 상황에서 안정성 있는 전환을 수행하기 위해서는 단계별로 서서히 전환해 나가는 전략이 필요하기 때문이다. 경찰통신망의 내부 현황과 경찰의 내부 정책에 맞춘 단계별 이행 모델을 수립해야 한다.

넷째, 전체 네트워크 구조를 단계별로 전환함과 함께 영역별 우선순위를 적용한 단계적인 전환 전략도 필요하다. 즉, 우선 네트워크 장비(라우터, 스위치, 방화벽 등)의 전환 계획을 수립하고, 다음으로 서버의 IPv6 전환계획을 수립한다. 그리고 마지막으로 응용서비스의 전환계획을 수립한다. 네트워크 장비의 경우 IPv6 지원 여부를 확인하여 교체 혹은 증설 여부를 판단하여야 하며, 서버 OS의 경우에도 교체 혹은 업그레이드 여부를 판단하여 수행하여야 한다. 응용서비스의 경우 종류가 많고 광범위하여 모든 애플리케이션의 개발 및 전환이 어렵기 때문에 주요 응용 서비스인 메일, 웹, DNS 등의 전환을 우선 고려한다.

다섯째, IPv6로 전환하면서 새로운 기술 및 서비스를 같이 도입하는 것이다. IPv6는 IPv4 와 비교할 때 이동성이나 QoS 등을 효과적으로 지원한다. 따라서 이행모델 수립 단계에서 이러한 장점들을 살릴 수 있는 기술의 도입이나 서비스의 도입도 같이 실시하면 IPv6로의 전환에 대한 효과를 배가 시킬 수 있을 것이다.

〈그림 26〉 국내 사례 시사점 도출



4. 해외 사례분석

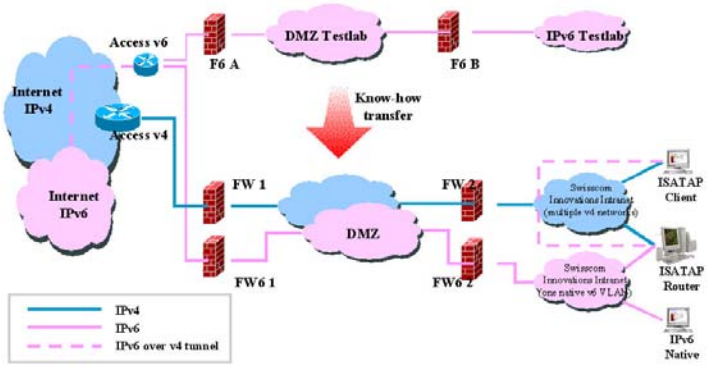
해외의 IPv6 이행모델 사례로는 스위스 swisscom의 "intranet transition to IPv6 이행모델"과 독일의 Műnster 대학의 IPv6 이행모델을 조사하고 분석하여 시사점을 도출하였다.

가. Swisscom의 IPv6 이행 전략

스위스의 swisscom은 자사의 Intranet을 IPv6로 전환하기 위하여 이행 모델을 수립하였다. 우선 이행 모델 수립에 앞서 swisscom은 현황 조사를 실시하였는데, 네트워크 장비들의 IPv6지원여부와 OS의 버전 등을 조사하고, 네트워크 실무자들을 인터뷰하였다. 그 결과, 네트워크를 구성하고 있는 라우터와 방화벽의 일부가 IPv6를 지원하지 않음을 발견하였다. 또한 네트워크 운영부서의 담당자들이 아직 IPv6의 보안성과 안정성에 대해 완벽하게 신뢰하지 못하고 있다.

따라서 swisscom은 단계별(1단계:ISATAP, 2단계:Small dual-stack island, 3단계:ISATAP제거) 이행 전략을 수립하였다. IPv6를 지원하지 않는 장비가 많기 때문에 한꺼번에 전체 네트워크를 Dual stack 하지 않고 이행 초기에는 ISATAP 솔루션을 이용하여 자동 터널링 하는 방법으로 IPv6 Application을 운영하며 점차 IPv6 Application을 늘렸다. 이후 Small dual-stack island을 구성하여 ISATAP과 병행하며 IPv6를 운영하고, dual-stack을 점차 확대하여 전체 네트워크를 dual-stack화 하고 ISATAP 솔루션을 단계적으로 제거하였다〈그림 27〉

〈그림 27〉 swisscom의 logical IPv6 network 구성도

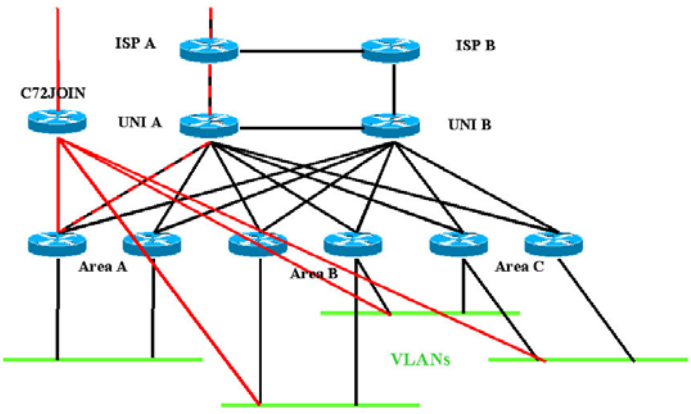


swisscom의 이행 모델 중에 주목할 만 한 것은 다른 여타 이행 모델들이 그랬듯이 swisscom도 IPv6 이행에 우선순위를 두었다는 것이다. 3개의 side로 우선순위를 구분했는데 첫 번째 순위로는 네트워크장비, 네트워크 설계 등이 해당되는 network side이고, 두 번째는 Server side로서 Sever의 OA 버전 등의 업그레이드가 여기에 해당한다. 세 번째는 Client side로 각각의 응용 서비스에 대한 IPv6 이행이 여기에 해당한다.

나. 독일 Műnster 대학의 IPv6 이행 모델

독일의 Műnster 대학은 매우 크고, 비교적 복잡한 네트워크를 갖고 있다. 특히 오랜 시간에 걸쳐 서서히 구축된 네트워크이기 때문에 부분적으로 오래전 네트워크기술을 여전히 사용하는 구간이 많고, 장비의 종류나 버전들도 매우 다양하다. IPv6가 지원되지 않는 장비도 많았으며, 기존 장비의 벤더가 IPv6를 지원하지 않는 경우도 있어서 장비를 업그레이드 할 것인지, 새로 구매할 것인지, 장비 벤더도 바꿀 것 인지 등에 대한 결정을 해야 했다. 장비뿐만 아니라 네트워크 기술도 ATM, FDDI, IDSN 등이 혼재되어 있어, 네트워크 전체를 한꺼번에 dual-stack 하는데는 많은 문제가 있다. 따라서 Műnster 대학은 IPv6 이행전략의 핵심을 IPv4를 손상시키지 않는 범위내에서 부분적으로 IPv6를 시작하되 이를 위한 방법으로 VLAN(802.1q)기술을 이용하는 것으로 결정하고 별도 라우터를 설치하여 VLAN과 VLAN 인터페이스를 설정하였다. 단, ATM 이나 FDDI처럼 VLAN 기술을 사용할 수 없는 경우에는 다양한 터널이나 터널브로커 등을 사용했다.

〈그림 28〉 Műnster 대학의 테스트베드 구성도



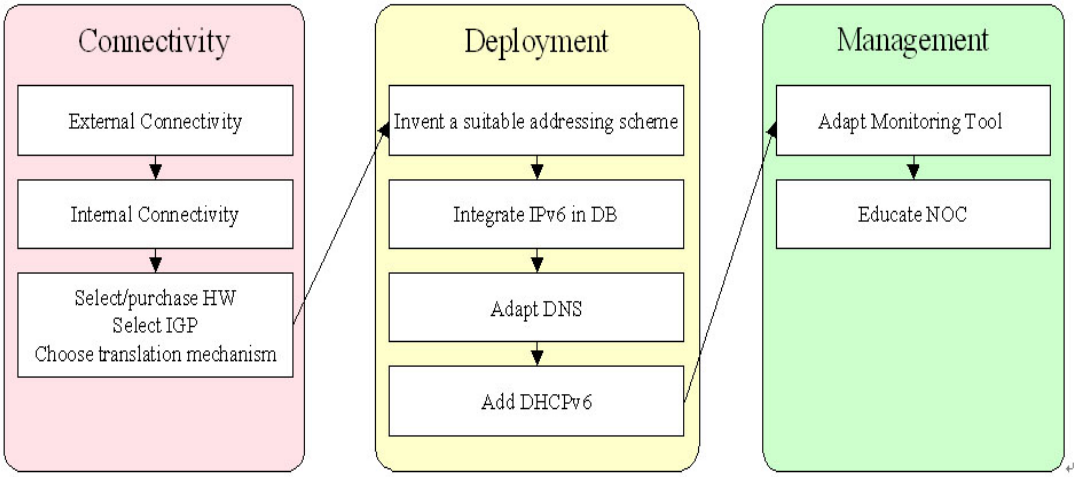
Műnster 대학의 IPv6 이행모델은 다음과 같다

- 1Step : VLAN을 위한 장비선택
- 2Step : 외부의 connectivity (6 to 4 tunnel을 이용하여 6wind에 연결)
- 3Step : Internal connectivity (듀얼스텍, tunnel broker, ISATAP)
- 4Step : IGP 선택 (OSPFv2/OSPFv3 multi topology)
- 5Step : DNS, IPv6 DB, DSCPv6 결정
- 6Step : 주소할당 (/48, /51, /55, /57)
- 7Step : Management tool 선택 (IPv4와 IPv6 모두 관리할 수 있는 장비선택)
- 8Step : 응용서비스 전환 (DNS, HTTP, FTP, SMTP, NTP, NNTP, IMPP 등)

다. 해외 사례의 시사점

국내 사례에서와 마찬가지로 해외 사례에서도 현황 파악의 중요성과 단계별 전환전략수립, 우선순위에 의한 이행 등의 중요성을 확인할 수 있었다. 특히 네트워크 규모에 따라 전환 전략의 차별화는 매우 중요하다. 해외 사례에서 살펴본 두 SITE는 규모가 크고 복잡한 구조의 네트워크로 구성되어 있었다. 이런 경우 IPv6 지원이 되지 않는 장비가 많고 오랜 기간에 걸쳐 네트워크가 구성되면서 여러 세대의 기술들이 혼재된 경우가 많아 한꺼번에 전체 네트워크를 dual-stack화 하기에는 무리가 있었다. 따라서 부분적인 dual-stack화를 시도하던지 터널링 기법을 이용한 전환을 시도하는 등의 방법으로 초기 전환 전략을 수립하였다. 경찰통신망도 비교적 크고 복잡한 네트워크라고 볼 수 있으므로 경찰통신망 현황에 맞는 단계별 이행 전략이 필요할 것이다. 위의 대부분의 사례에서 나타난 IPv6 전환이행 절차를 보면 다음 〈그림 29〉과 같다.

〈그림 29〉 IPv6 이행 절차



위에서 본 바와 같이 한 순간에 전체 네트워크를 dual-stack으로 전환하는 것은 쉽지 않다. 따라서 적절한 IPv6 전환메커니즘이 필요한데, 해외사례를 통해 본 전환메커니즘 선택 시 고려사항은 다음과 같다

- 확장성, 보안성, 성능, Addressing 고려
- 호스트와 라우터 요구사항, 애플리케이션 요구사항
- 사용 편리성, 관리 편리성
- 멀티캐스트 지원 여부

5. IPv6 장비 관련 업체 동향

국내외 IPv6 장비 관련업체의 현재 제품들의 조사한 것으로 라우터, 스위치, 서버등 주요기능 및 특징 등을 보여준다.

가. 라우터

〈표 13〉 국산 라우터

제조사	모델명	주요기능 및 특징	출시시기
모다정보통신	U-Road 2000	o IPv6/IPv4 동시 지원 Fast Hand off 지원	'05.12
	U-Road 1000	o IPv4/IPv6 동시지원 Fast Hand off 지원	'05.12
머큐리	RUSH-1000W	o IPv4 IPv6 Dual Stack Router로 Ethernet과 전용선 V 35 프로토콜을 지원하며 무선랜도 지원 가능함	'05.06
삼성전자	GWIM	o 삼성전자 OS7400 GWIM IPv4는 기 판매 IPv6 Router는 개발	'05.12
CoreBell	IPv4 IPv6 표준 라우터 플랫폼	o NP 기반의 기가비트 고속 라우터	'05.12
애드팍 테크놀러지	AP4820	o ATM, 매트로이더넷, POS, HSSI, V.35 Serial 등 다양한 WAN 인터페이스	'01
	AP5840	o IPv4/IPv6/IPSec/IPv6VPN 지원	'04
	AP5850	o 로드밸런싱, 장애복구 위한 VRRP 지원	'04

〈표 14〉 외산 라우터

제조사	모델명	주요기능 및 특징	출시시기
시스코 시스템즈	Cisco catalyst 6500	o 통신사업자 및 대규모 기업용 백본 스위치	'03.10
	Cisco catalyst 4500	o 중형급 백본 스위치	'04.01
	Cisco catalyst 3750	o 고정 구성형 Intelligent Ethernet 스위치	'05.03
	Cisco catalyst 3560	o 고정 구성형 Intelligent Ethernet 스위치	'05.03
LG 히다찌	AX6300S 시리즈	o 최대 192G 백플레인 및 64 포트의 10G 이더넷을 제공하는 IPv4/IPv6 백본 스위치	'07.01
	AX6700S 시리즈	o 최대 1.15Tbps 백플레인 및 64 포트의 10G 이더넷을 제공하는 IPv4/IPv6 백본 스위치	'07.01
	AX3600S 시리즈	o 이더넷을 제공하는 1U 사이즈의 레이어 3 IPv4/IPv6 워크그룹 스위치	'06.03
	AX2400S 시리즈	o 10G 이더넷을 제공하는 1U 사이즈의 레이어 2 워크그룹 스위치	'06.03
	AX7800S 시리즈	o 최대 768G 백플레인 및 32 포트의 10G 이더넷을 제공하는 IPv4/IPv6 백본 스위치	'06.03
	GS3000-20/40	o 최대 96G 백플레인 및 160 포트의 1G 이더넷을 제공하는 IPv4/IPv6 미드레인지 스위치	'03.10
	GS4000-80/160/320	o 최대 768G 백플레인 및 32 포트의 10G 이더넷을 제공하는 IPv4/IPv6 백본 스위치	'03.10

주니퍼 네트웍스	TX	o IPv4/IPv6 듀얼스택 라우터 o Configured 터널링 지원 o Static, RIPng, OSPFv3, IS-IS, MP-BGP지원 o 성능 : 256Tbps H/W 처리	'04.12
	ERX320	o IPv4/IPv6 듀얼스택 라우터 o Configured 터널링 지원 o Static, OSPFv3, MP-BGP지원 o 성능 : 320Gbps H/W 처리 o IPv6 BRAS	'05.10
	T640	o IPv4/IPv6 듀얼스택 라우터 o Configured 터널링 지원 o Static, RIPng, OSPFv3, IS-IS, MP-BGP지원 o 성능 : 640Gbps H/W 처리 o IPv6 Ready Logo Phase I 취득	'02.05
NEC	IX2010	o IPv4/IPv6 듀얼스택 라우터	'03.01
시스코 시스템즈	Cisco CRS1	o 통신사업자 백본급 라우팅 서비스 장비	'05.06
	Cisco 12800	o 통신사업자 멀티서비스 라우팅 서비스 장비	'03.10
	Cisco 7600	o 에지용 멀티서비스 통합용 코어라우터	'03.10
	Cisco 7500	o 에지용 멀티서비스 라우터	'02.02
	Cisco 3800/2800/1800	o 기업용 멀티서비스 통합 라우터	'04.08
	Cisco 800	o 소호 및 소규모 사업자용 라우터	'02.02
LG 히다찌	AX7800R 시리즈	o 최대 768G 백플레인 및 32 포트의 10G 이더넷을 제공하는 IPv4/IPv6 백본 라우터	'06.05
	GR2000-1B/2B	o 1U 사이즈에서 기가이더넷 인터페이스 및 4 기가 백플레인을 제공하는 고성능 IPv4/IPv6소형 라우터	'01.03
	GR2000-S/H 시리즈	o 90G 백플레인및 40Mpps 의 성능을 제공하는 시리얼,이더넷,기가이더넷,POS 인터페이스 등을 제공하는 고성능 라우터	'01.03
	GR4000-80/160/320	o 최대 768G 백플레인 및 32 포트의 10G 이더넷을 제공하는 IPv4/IPv6 백본 라우터	'03.10

나. 서버

〈표 15〉 국산 서버

제조사	모델명	주요기능 및 특징	출시시기
아이엠넷피아	exMove	o Mobile IPv6 기능지원	'05.11
위즈정보기술	SPX2000i	o 방화벽 VPN 등	'06.10

다. 스위치

〈표 16〉 국산 스위치

제조사	모델명	주요기능 및 특징	출시시기
삼성전자	GSIM	o IPv4 L3 Switch로 기 판매 IPv6는 개발 중	'05.12
다산네트웍스	V5224G	o IPv4/IPv6 듀얼스택 L3 중,소형 스위치 o 16Port + 8 combo 기가스위치 지원	'06.09
	V5724G	o IPv4/IPv6 듀얼스택 L3 중,소형 스위치 o 24Port 기가스위치 지원	'06.09
	V5424G	o IPv4/IPv6 듀얼스택 L3 중,소형 스위치 o 24Port 기가스위치 지원	'06.09
	V6324F	o IPv4/IPv6 듀얼스택 L3 중,소형 스위치 o 24Port FX + 4Port 기가스위치 지원	'06.09
	V5xxx 시리즈, V6xxx 시리즈	o L2, L3 gigabit 이더넷 스위치	'07

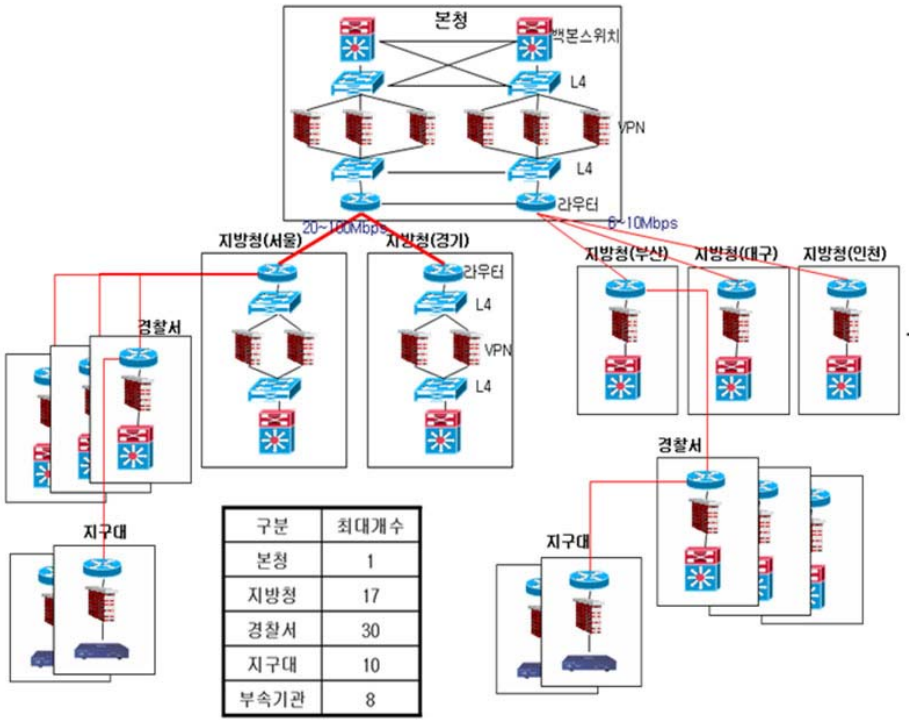
〈표 17〉 외산 스위치

제조사	모델명	주요기능 및 특징	출시시기
시스코 시스템즈	Cisco catalyst 6500	o 통신사업자 및 대규모 기업용 백본 스위치	'03.10
	Cisco catalyst 4500	o 중형급 백본 스위치	'04.01
	Cisco catalyst 3750	o 고정 구성형 Intelligent Ethernet 스위치	'05.03
	Cisco catalyst 3560	o 고정 구성형 Intelligent Ethernet 스위치	'05.03
LG 히다찌	AX6300S 시리즈	o 최대 192G 백플레인 및 64 포트의 10G 이더넷을 제공하는 IPv4/IPv6 백본 스위치	'07.01
	AX6700S 시리즈	o 최대 1.15Tbps 백플레인 및 64 포트의 10G 이더넷을 제공하는 IPv4/IPv6 백본 스위치	'07.01
	AX3600S 시리즈	o 이더넷을 제공하는 1U 사이즈의 레이어 3 IPv4/IPv6 워크그룹 스위치	'06.03
	AX2400S 시리즈	o 10G 이더넷을 제공하는 1U 사이즈의 레이어 2 워크그룹 스위치	'06.03
	AX7800S 시리즈	o 최대 768G 백플레인 및 32 포트의 10G 이더넷을 제공하는 IPv4/IPv6 백본 스위치	'06.03
	GS3000-20/40	o 최대 96G 백플레인 및 160 포트의 1G 이더넷을 제공하는 IPv4/IPv6 미드레인지 스위치	'03.10
	GS4000-80/160/320	o 최대 768G 백플레인 및 32 포트의 10G 이더넷을 제공하는 IPv4/IPv6 백본 스위치	'03.10

제4장 경찰 IPv6 도입

현재 경찰 IP 네트워크 구조는 아래의 그림과 같다. IPv6 망 설계를 위해서는 아래의 네트워크 구조를 바탕으로 계위를 구분하는 것이 우선적으로 필요하다. 또한 Subnet 설계에 필요한 개수는 본청, 지방청, 경찰서, 지구대 별로 최대 개수를 적용한다.

〈그림 30〉 경찰 Network 구조



구분	최대개수
본청	1
지방청	17
경찰서	30
지구대	10
부속기관	8

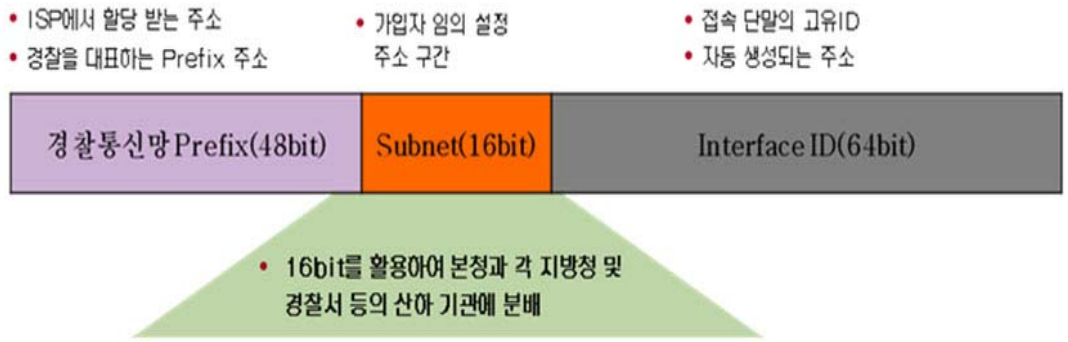
경찰통신망의 Subnet 설계는 계층화 구조를 이루는 각 계층을 어떻게 나눌 것인가에 대한 기본 정책이 필요하다. 각각의 최대 개수가 곧 계층별 필요한 Subnet의 개수가 된다. 〈표 18〉은 경찰 IPv6 망을 이루는 각 계층별 최대 개수를 나타낸다.

〈표 18〉 전국 경찰 Subnet 최대 개수

구 분	최대 개수	비 고
본 청	1	
지방청	17	
부속기관	8	부속기관
경찰서	30	최대 경찰서계 수
지구대	10	직할대계, 기타

경찰통신망의 IPv6 주소설계는 안정적으로 확보 가능한 최소 48bit Prefix을 기준으로 설계하였다.

〈그림 31〉 경찰 IPv6 주소 체계



위의 그림은 경찰 IPv6 주소 체계를 나타낸 그림으로, 총 128bit IPv6 주소 구간 중 처음 48bit는 경찰을 대표하는 주소로 ISP 변경 시 라우터의 주소 수정 작업이 필요한 구간이다. ISP로부터 배정받은 Prefix 다음의 16bit는 Subnet구간으로 실제 경찰 IPv6 주소 설계가 이루어지는 부분으로 가입자가 임으로 설정 가능하다. 하위 64bit는 접속 단말의 고유 ID로서 자동 생성되는 주소이다. Subnet 할당은 IPv6 주소설계의 핵심으로 우선 경찰통신망의 구조를 정의하고, Subnet 최대 개수를 충분히 수용할 수 있도록 bit를 할당한다.

제1절 경찰 IPv6 네트워크 구조

본보고서에서는 두 가지 IPv6 망 구조를 제안한다. 첫 번째는 수평구조이다. 지방청, 경찰서, 지구대를 같은 계위로 구성하는 방안이고, 두 번째는 수직구조로 경찰청à지방청à경찰서à지구대의 형태로 계위로 구분하여 구성하는 방안이다.

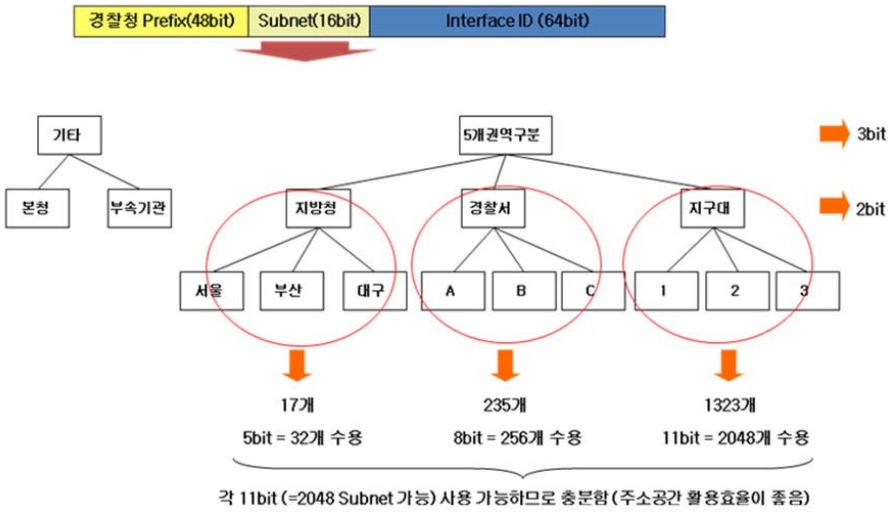
가. 경찰 IPv6 네트워크 구조(안) : (부분적) 수평구조

지방청-경찰서-지구대를 수평으로 배치하는 구조로서, 본청과 지방청5개권역을 나누고, 5개권역 아래의 지방청, 경찰서, 지구대를 수평구조로 설계하는 방안이다.

아래의 그림은 Subnet(16bit)중 상위 3bit를 기타(본청, 부속기관), 5개권역을 구분하는데 할당하고, 5개권역 예하의 각각의 지방청, 경찰서, 지구대를 구분하기 위한 2bit를 할당한다. 상위 5bit를 제외한 나머지 부분은 수평구조 이므로 나머지 11bit를 할당한다. 11bit중 상위 5bit는 지방청 구분하는데 사용하고, 5bit를 포함한 상위 8bit를 경찰서를 구분하는데 사용하고, 8bit를 포함한 11bit를 지구대를 구분하는데 사용한다.

각 11bit(=2048 Subnet 가능)를 사용 가능하므로 주소공간 활용 효율이 좋다.

〈그림 32〉 수평구조

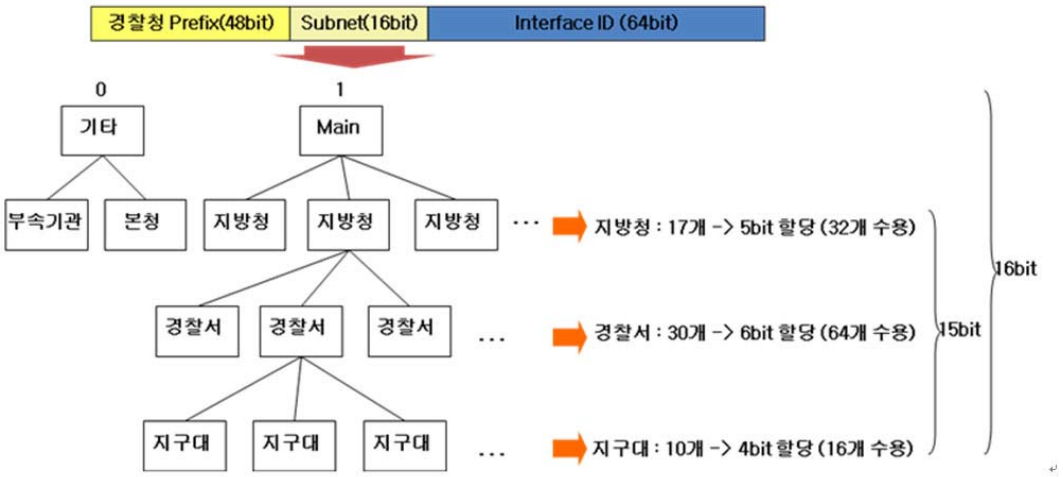


나. 경찰 IPv6 네트워크 구조(안) : 수직구조

현재 경찰 네트워크 구조를 그대로 유지하는 구조로, 본청과 Main을 구분하는 1bit 할당하고, 나머지 15bit를 가지고 지방청, 경찰서, 지구대 순으로 계층적으로 할당하는 방안이다. 아래의 그림은 수직구조로 경찰 네트워크를 설계한 것으로, 지방청 최대 개수가 17개 이므로 5bit(32개 수용)를 할당하고, 경찰서 최대 개수가 30이므로 6bit(64개 수용) 그리고 지구대의 최대 개수가 10이므로 4bit(16개 수용)를 Subnet을 할당한다.

이러한 수직구조의 가장 큰 특징은 IP로 해당 지역 및 경찰서 지구대가 어디 있지 확인하기가 용이하다.

〈그림 33〉 수직구조



다. 수평구조와 수직구조의 비교

아래의 표는 수평구조와 수직구조를 비교한 것으로 수평구조의 경우 청-서-지구대를 논리적으로 동등한 계위를 가지며, 수직구조의 경우 각각의 계위를 3단계로 나누는 것이다. 수직구조의 계위는 기본적으로 IP망 물리적 구조를 따른다.

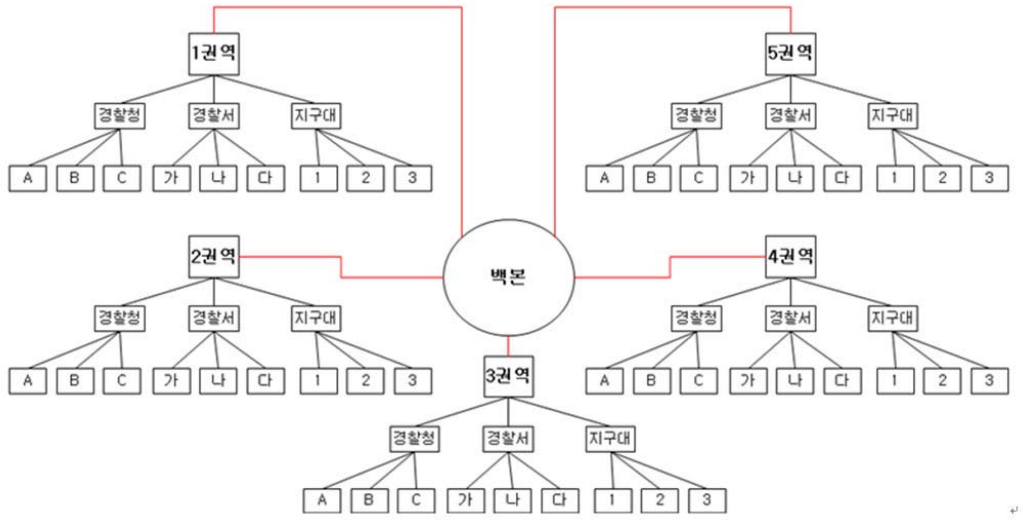
〈표 18〉 수평구조 VS. 수직구조 비교표

구 분	수평 구조		수직 구조	
형 태	청-서-지구대의 수직 계층 구조를 무시하고 논리적인 IP 망을 새롭게 구성		청-서-지구대의 수직 계층 구조를 그대로 반영하는 구조	
Routing Path	O	• Data 송수신 End-to-End 경로가 수직 구조에 비해 단순해짐	X	• 수직 구조이므로 End-to-End 경로상의 hop 수가 상대적으로 많아짐
주소의 사용 효율	O	• 16bit 거의 전체를 한 계위에서 사용 가능하므로 주소 사용 효율이 매우 좋음 • 분할과 통합에 유리하고, 여유율 활용 가능성이 증대된다. • 주소 축약사용이 가능한 구조임	X	• 계층 구조를 위해서 16bit 를 나누어야 하므로 주소 사용 효율이 매우 떨어짐
Management/ 보안	X	• 청-서-지구대의 구조를 무시하는 형태이므로 IP 주소를 통해 개인 IP node의 계층적 소속을 알기 어려움 • 외부-내부 IP node 까지의 경로가 최소의 계층으로 단순하므로 사이버침해도 비교적 용이함	O	• 청-서-지구대의 구조를 그대로 반영하는 구조이므로 IP 주소를 통해 개인 IP node의 계층적 소속을 알 수 있음 • 외부-내부 IP node 까지의 경로가 계층화가 이루어져 있으므로 각 계층별 보안시스템 구축 시 사이버침해도 그만큼 어려워짐

제2절 경찰 IPv6 네트워크 구조(안)

두 가지 안을 비교했을 때, 수평구조는 보안적인 측면에서 사이버 침해에 용의한 측면이 있으나, 경찰 내부망의 경우 외부망과 분리되어 있고, 라우팅 경로의 단순화 및 주소 설계의 효율성이 좋고, 추후 확장에 용의하므로 부분적 수평구조를 경찰망에 적용하는 것이 적합하다. 아래의 〈그림 34〉은 전국을 5개 권역으로 구분하여 IPv6 네트워크를 설계한 것이다. 백본을 중심으로 5개권역으로 나누고, 각각의 권역별 지방청, 경찰서, 지구대가 동등한 계위에 존재하게 된다. 차후 USN 및 최하위 단말이 증가할 때 수직구조에 비해 상대적으로 주소할당 효율이 좋으므로 이에 대비할 수 있는 구조 이다.

〈그림 34〉 5개 권역에 부분적 수평구조 적용(예)



제3절 경찰 통신망 IPv6 전환 전략

경찰통신망이 ALL IP 환경으로 진화됨에 따라 이에 통신망 운용을 안정적으로 지원하기 위해서는 계획 단계에서 정확한 추진방침이 마련되어야 한다. 따라서 다음의 다섯 가지 기본 추진방침에 따라 망 운용을 한다.

- 단계적 전환
- 보안
- 상호 운용성
- 표준기반
- 최소의 비용

1. 단계적 전환

IPv6 전환으로 인한 위험요소를 최소화하기 위하여 단계적 전환이 이루어져야 한다는 것이다. IPv6의 기술적 성숙도는 이미 매우 높다고 할 수 있고 실제 정보통신 환경에서의 기술 검증 및 가용성 검증도 활발히 이루어 지고 있지만 실제 업무망에 적용한 경우는 많지 않아 아직 찾기 힘들어 IPv6 이행을 확실하게 검증할만한 성공모델이 부족한 실정이다. 따라서 경찰통신망의 IPv6 이행은 관련 기술의 신뢰성, 성숙도를 기반으로 기존 업무 수행 체계와 환경에의 영향을 최소화 되도록 단계적인 전환이 이루어져야 한다.

2. 보 안

두번째 추진 방침으로는 보안 문제의 해결이다. 정보통신망에서의 보안은 정보체계 구축과 운용에 있어 가장 기본적인 요구사항이라 할 수 있다. 보안 문제에 대해서는 크게 3가지 관점에서 접근할 수 있는데 IPv4 기반의 보안성을 IPv6에서도 유지해야 한다는 점, IPv6 프로토콜 자체적으로 내재하고 있는 보안문제 해소, IPv6 전환 기술 적용 시 나타날 수 있는 보안 문제에 대한 대응 방안이 마련 되어야 하는 것이다. 경찰통신망의 IPv6 이행을 위한 수많은 정보체계 및 네트워크 자원의 수정, 변경, 교체 시 현재 유지되고 있는 보안성을 훼손하거나 방해하지 말아야 하고, IPv6의 ICMPv6, Anycast, 소스 라우팅에서의 보안문제, Dual stack/Tunnel/Translation 등에 서의 보안 문제에 대응 방안을 마련하여야 한다.

3. 상호 운용성 유지

세 번째로는 IPv6 전환으로 인한 상호 운용성 침해를 최소화해야 한다는 것이다. 즉, 경찰통신망내의 다양한 정보체계들의 상호 운용성이 보장되어야 한다는 것이다. 현재 네트워크 기반 프로토콜인 IPv4와 IPv6는 기본적으로 상호 호환이 되지 않는다. 따라서 IPv6 이행을 적용할 시에 정보체계, 네트워크간 상호 운용성 영향을 미칠 수 있다. 이러한 악영향을 최소화하기 위한 전환 전략이 필요하다. 이때 고려사항으로는 터널기법의 최적적용을 통한 데이터 교환, 서버와 클라이언트 동시전환, 기술적 복잡도와 그에 따른 비

용증가의 부담을 갖고 있는 Translation 기법의 최소화 등이 있다.

4. 표준 기반

네 번째로는 IPv6 관련 표준/규격에 기반한 전환이 이루어져야 한다는 것이다. 향후의 효율적이고 체계적인 유지보수 및 성능개량을 위해서라도 특정/고유 기술의 적용을 최소화하고 표준/규격에 기반한 기술 도입과 구축/운용이 이루어져야 한다. 이를 통해 새로운 기술 적용의 위험 및 비용을 최소화하고 상호 운용성 정도를 극대화 할 수 있다.

5. 최소 비용

다섯 번째로는 IPv6 전환에 소요되는 비용을 최소화 하는 것이다. 경찰통신망 구성 시스템의 수명 주기에 맞춘 IPv6 지원 시스템/장비의 도입으로 전환비용을 최소화하고 효과적인 전환 모델의 적용을 통한 시행착오의 최소화로도 전환비용을 줄일 수 있다. 따라서 전환 모델 시뮬레이터 등을 통해 검증하고, IPv6 인프라에 적요할 장비, 솔루션, 응용시스템 등을 시험하고 검증할 필요가 있다. 또한 경찰통신망을 구성하고 있는 장비와 어플리케이션들의 정확한 현황 파악을 통해 IPv6 전환에 필요한 장비의 대체, 업그레이드 요구사항에 대한 정확한 조사와 분석이 필요하다.

6. 경찰통신망 IPv6 이행 로드맵

앞의 경찰통신망 IPv6 전환전략의 기본 방침에서 가장 첫 번째로 강조한 내용이 단계적 전환이다. 본 보고서에서는 경찰통신망의 IPv6 전환을 준비단계, 진입단계, 본격이행단계, 고도화 단계로 구분하여 단계별 이행 내용을 담은 로드맵을 제시한다. 단, 응용시스템의 IPv6 전환은 IPv4 기반응용시스템을 IPv6로 전환하는 경우와 신규 서비스를 IPv6로 개발하여 도입하는 경우의 두 가지 측면에서 접근하였다. 전자의 경우에는 경찰통신망에서의 중요도를 고려하여 주요 서비스 목록을 만들고 IPv6로 전환하는 우선순위를 결정하여야 한다. 다음의 표는 경찰통신망의 IPv6 이행 가상 로드맵을 나타내는 표이다.

〈표 19〉 경찰통신망 IPv6 이행 로드맵

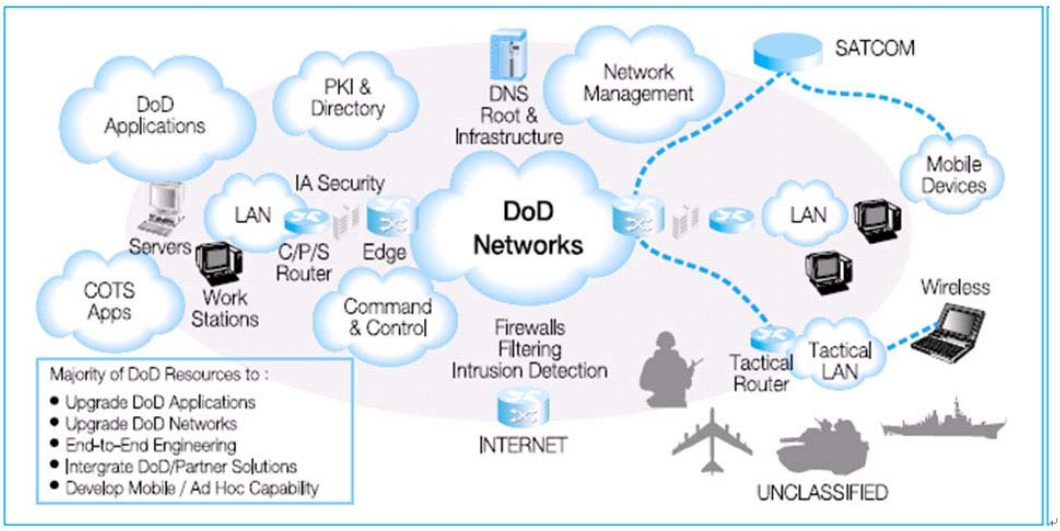
단계	준비단계 (2007년)	진입단계 (2008~2010년)	본격이행단계 (2011~ 2016년)	고도화단계 (2017년~)
이행 내용	- 시험망 구축 및 운용 - 듀얼스택 네트워크 장비의 안정성 및 전환기술 시험 - IPv6로 전환된 응용체계의 성능 및 기능 시험	- 경찰통신망 각 사업소의 점진적인 IPv6 전환 - 경찰통신망 응용서비스의 IPv6 전환 시작 - IPv6용 신규장비들의 도입으로 듀얼스택 환경의 지원기반을 점진 확대	- 경찰통신망 응용서비스의 IPv6 전환 완료 - 경찰통신망 백본의 IPv6 전환 완료	- 경찰통신망의 native IPv6로의 전환 완료 - IPv6 - value added 응용 시스템구축의 활성화 및 고도화 추진

7. 경찰통신망 IPv6 이행 이슈

미 국방성(DoD)는 미래 군사력 운용 기반인 GIG(Global Information Grid) 환경에서 NCW(Network Centric Warfare) 구현을 위한 핵심 요소로서 IPv6 전환을 추진해 왔으며 2003년 10월 이후부터 모든 GIG 자산에 IPv6가 가능하도록 개발하였다. 〈그림 35〉은 DoD의 IPv6 전환 대상을 나타낸 것이다. DoD가 IPv6로의 전환을 추진하는 이유는 IP가 포괄적 군사 네트워크 GIG(Global Information Grid)를 통한 정보처리 상호운용의 기반이기 때문이다. DoD는 세계 각지의 미군 거점 및 전선 등을 인터넷으로 연결하는 '글로벌 인포메이션 그리드(GIG)'를 구축 중이다. 미군들에게 소형 정보 단말기를 제공해 전투 및 작전행동 상황을 실시간으로 전달하는 '인터넷 전투'를 지향하고 있는 것이다.

IPv6는 GIG 하에서 센서, 플랫폼, 모바일, Wireless들 간에 상호 접속을 가능하게 해줌으로써 네트워크 중심의 임무수행이 가능하게 한다. 즉, DoD는 IPv6 조기 도입을 통해 무한한 주소와 보안성, 이동성 등을 얻음으로써 군사의 각 제대 및 군의 최소단위인 병사 개개인까지 상호 통신을 가능하게 할 계획이다.

〈그림 35〉 미 국방성(DoD) IPv6의 전환대상



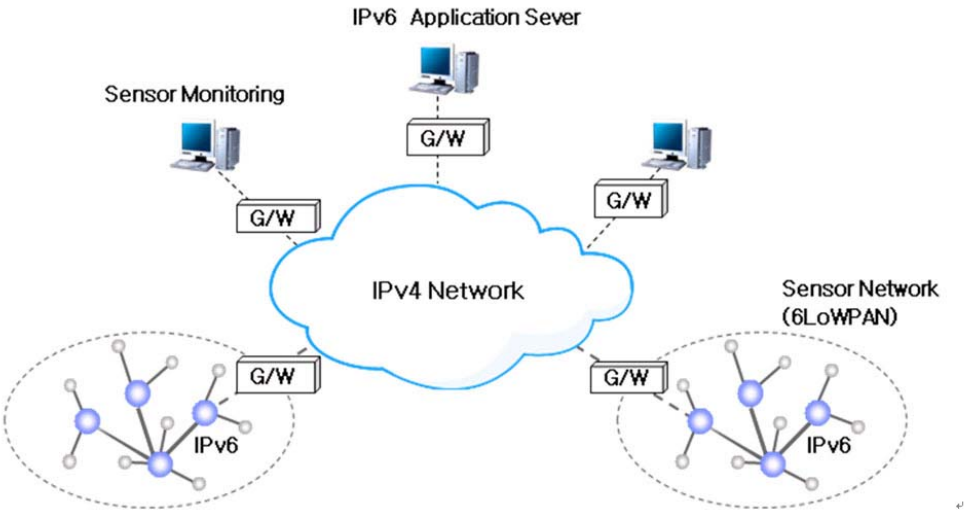
DoD IPv6 전환 핵심 부서인 IPv6 테스크포스(Task Force)의 IPv6 도입과 관련최종보고서에 따르면, 장기적으로 볼 때 IPv6 도입이 필수적이 나 단기적으로는 IPv4에서 IPv6로의 전환과정에서 안전성이 떨어질 수도 있기 때문에 조기 도입이 필요한 것은 아니다라고 제시하고 있다.

이처럼 특정분야만 IPv6화 했을 경우 시너지 효과가 없을 뿐더러 효율이 저하될 것이다. 이는 또한 문제를 유발 시키는 요소가 될 수도 있다. 이러한 이유로 과도기 대안으로 IPv6를 일부분에 시행 모델로는 적합하지 않다.

IPv6 이행 전략 모델은 망의 IPv6화, 단말의 IPv6화, 응용서비스의 IPv6화, 운영체계 IPv6화가 모두 이루어져야만 시너지 효과가 증대될 것이다. 그렇지만 가능한 새로 도입되는 자원은 IPv6 수용할 수 있는 인증체계를 구비토록 하고, IPv6 망 및 주소체계를 선택적으로 확보하여 IPv6 기반 응용서비스의 조기도입에 기여한다.

아래의 〈그림 36〉에서와 같이 인프라는 IPv4를 유지하고 서비스 구간과 서버만 IPv6를 도입하는 부분적인 IPv6 도입 방안을 고려해 볼 수 있다.

〈그림 36〉 IPv6의 부분적으로 도입



제4절 경찰 VoIPv6

경찰 전화번호 설계에 앞에서 “공공기관 VoIPv6망 참조 모델” 기반으로 하여 기본적인 구성요소 및 구축에 필요한 사항을 분석하여 경찰청 VoIPv6 기본 모델 설계에 참고한다.

1. 공공기관의 VoIPv6 참조모델 v2.0 분석

공공기관 VoIPv6 참조모델은 정부기관에 VoIPv6 시스템 도입을 지원하는 도구로 사용자 시스템 구축에 필요한 다음의 사항을 정의한다.

경찰 VoIPv6 음성전화, 영상전화, 부가 서비스 제공을 위한 사용자 측 구성요소를 정의

- 신호프로토콜, 권장 VoIP 코덱, 음성데이터 전송 기술, VoIP 정보 보호 기술과 기타 제공서비스 제공 기술을 정의하고 해당 표준 권고
- VoIPv6 와 VoIPv4 혹은 VoIP와 PSTN간 연동 방법 등 정의
- 영상 서비스를 활용한 영상감지, 영상교육 등 다양한 영상 부가서비스 제시
- 음성전화와 영상 전화 품질 기준 및 품질 관리를 위한 방법 권고

가. 공공기관 VoIPv6 참조모델 용도

1) 공공기관 VoIPv6 참조모델에 정의된 표준 프로파일을 수용함으로써, 제품간 호환성을 유지하는데 목적이 있다.

2) 사용자 VoIPv6 시스템 사용 및 구축 편의성, 서비스 안정성을 확보

- 일관성 있는 사용자 인터페이스 제공 등을 통해 VoIPv6 시스템 이용 편의성 제공 및 시스템 구축 효율성 증진
- 서비스 설계 단계부터 보안을 고려하여 보다 안전한 VoIPv6 서비스 구축

3) 조직의 VoIPv6 자원 관리에 활용

- 참조모델에 따른 체계적인 VoIPv6 제품 관리
- 공공기관의 VoIPv6 관련 신기술 도입 지원

4) VoIPv6의 품질 관리

- 참조모델의 품질 기준을 만족시키는 서비스 제공을 유도하고 참조모델 기반의 품질 관리

5) VoIPv6 통신망 구축 및 관리에 활용

- 음성, 영상, 인터넷 통합 망 설계 및 구축 정보 활용
- 안정된 통합서비스 제공을 위한 품질측정 방안 정보 제공

나. VoIPv6 서비스를 위한 구성 요소

아래의 표는 공공기관 VoIPv6 서비스를 위한 구성 요소 중 사용자 구성 요소들을 나타낸 것이다.

〈표 20〉 음성전화 서비스 구성 요소

구 분	구성 요소	구성 요소 설명
사용자 측 단말	유선 IP전화기	전화망과 같은 회선 교환망 대신에 데이터 패킷망을 통하여 음성통화를 할 수 있도록 IPv6 인터넷 프로토콜이 탑재되어 있는 전화기
	무선 IP전화기	무선랜(WLAN) 기술을 이용하여 무선으로 음성통화를 제공하는 IP전화기
	소프트폰	PC나 PDA상에서 구동되는 프로그램을 이용하여 음성통화를 제공하는 소프트웨어 형태의 IP전화기
	단독형 액세스 게이트웨이	개인 사용자를 위하여 VoIPv6와 PSTN을 연결하는 장치로 FAX Relay 기능 등이 구현되어 있음
사용자 측 서버 시스템	집합형 액세스 게이트웨이	복수의 사용자를 위하여 VoIPv6와 PSTN을 연결하는 장치로 FAX Relay 기능 등이 구현되어 있음
	IP-PBX	IPv6 기반 네트워크에서 VoIP를 사용할 수 있도록 한 사설교환기로 다양한 PBX 기능을 지원함
	신호 전환 장치	SIP, H.323, MGCP 등 서로 다른 호간 연동을 수행하는 장치
	SIP 서버	VoIPv6 서비스를 위한 SIP 신호 연결, 제어, 관리 등을 동적으로 수행하는 장치

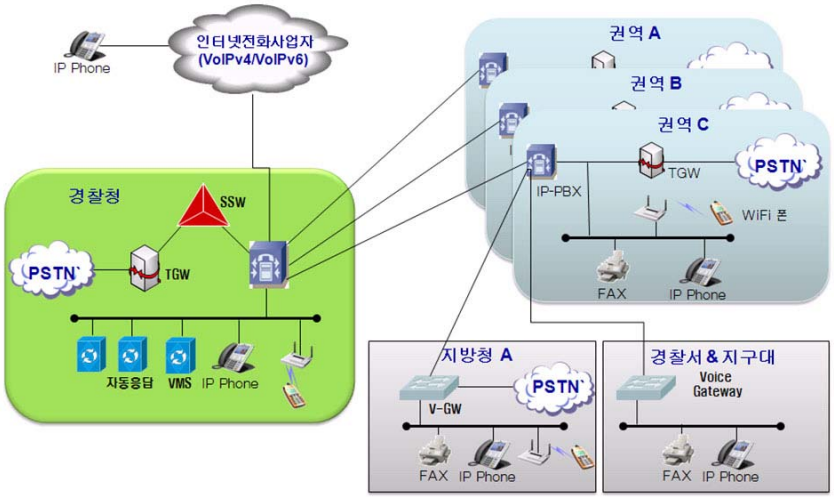
출처 : 공공기관 VoIPv6 참조모델 v2.0, 한국정보사회진흥원, 정보통신부

VoIPv6 서비스를 위한 구성 요소는 음성전화 서비스 구성요소와 영상서비스 구성요소, 네트워크 구성요소로 나누어져 있다. 경찰청의 경우 음성과 영상 망을 분리하는 형태로 구축되어 있기 때문에 주로 음성 서비스 구성요소를 바탕으로 경찰 VoIPv6 적용 모델을 설계하였다.

2. 경찰 VoIPv6 적용 모델

공공기관의 VoIPv6 참조 모델의 정의에 따라 경찰전화망 VoIPv6 적용 모델을 〈그림 35〉과 같이 정의한다.

〈그림 37〉 경찰전화망 VoIPv6 구성 모델



위의 그림은 경찰전화 백본망을 통해 각각의 지방청이 연결되며, 인터넷전화사업자(ITSP)의 경우 경찰청 IP-PBX 또는 백본망을 통하여 연결된다. 또한 각각의 권역의 IP-PBX에서 지방청, 경찰서, 지구대의 가입자를 수용한다. 각각의 권역 IP-PBX는 경찰청 IPT 시스템과 연동되어 있으며, 권역에는 해당 지방청 및 경찰서, 지구대가 수평구조로 각각 IP-PBX, Voice gateway 장비로 연동 될 것이다. 또한 PSTN의 경우 지방청까지는 자체적으로 연동하는 형태로 구성하는 것이 바람직하다. 왜냐하면 상위 IPT장비들의 폭주나 단절상태에서 타 지방청이나 경찰서와 연결할 수 있는 수단이기 때문이다.

제5장 경찰 VoIP 번호 체계 설계

제1절 주요이슈

VoIP 상호 연동에 있어서 고려 사항은 다음과 같다.

- 이기종 IPT 시스템간의 상호연동성 문제 (장비간 연동)
- 타 망과의 연계 문제 (VoIPv6 ßà VoIPv4, PSTN)
- 기존 PSTN 장비와 IPT 장비간의 연동 문제 (VoIP ßà PSTN)

1. 이기종 IPT 시스템간의 상호 연동성 문제

가. IPT 상호연동성의 개념

다양한 시스템간에 사용자의 보안정책을 유지하면서 인터넷전화서비스를 제공하기 위한 시스템들 상호간에 연동을 말한다.

나. IPT간 상호 연동

IPT와 상호연동하는 장치는 타 IPT, TG, 및 IP-PBX가 되며, 필요에 따라 단말(Terminal)도 상호 연동할 수 있다. IPT는 인터넷 통신망의 핵심이 되는 코어(Core) 호처리 시스템이라 할 수 있다, 따라서, 이기종 벤더 장비간의 연동에 있어 호환이 잘되도록 IPT 상호 연동성에 대한 기준이 마련되어야 한다.

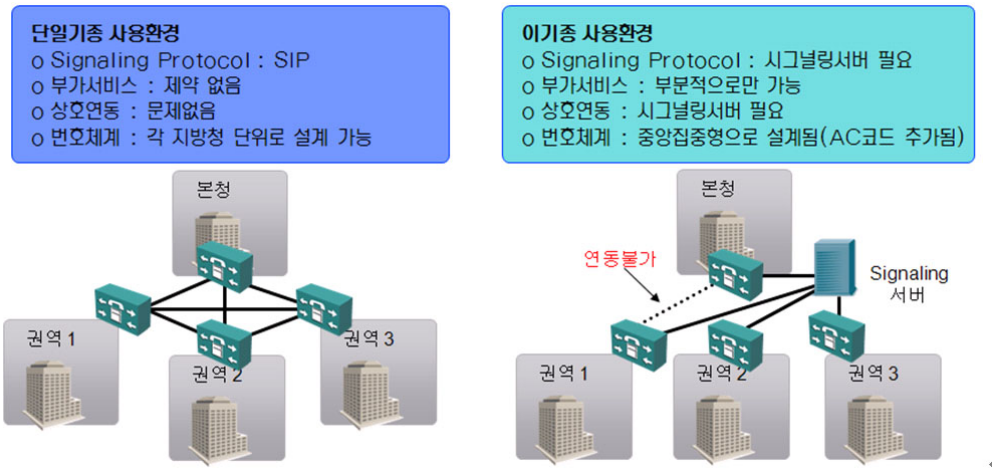
다. IPT간 상호 연동성 문제

전국경찰에 동일한 벤더의 IPT 시스템이 도입되기 힘들기 때문에 IPT 시스템간의 상호 연동성 문제를 고려해야 한다. 다음 그림은 “이기종 IPT 시스템”으로경찰전화망을구축

시" 문제점을 보여 준다.

특히 이기종 IPT 시스템간 연동이 안 될 경우 추가적이 시그널링 서버가 필요하게 되고 이 시그널링 서버를 통해 호가 전달되기 때문에 추가적인 액세스 코드 사용이 불가피하다.

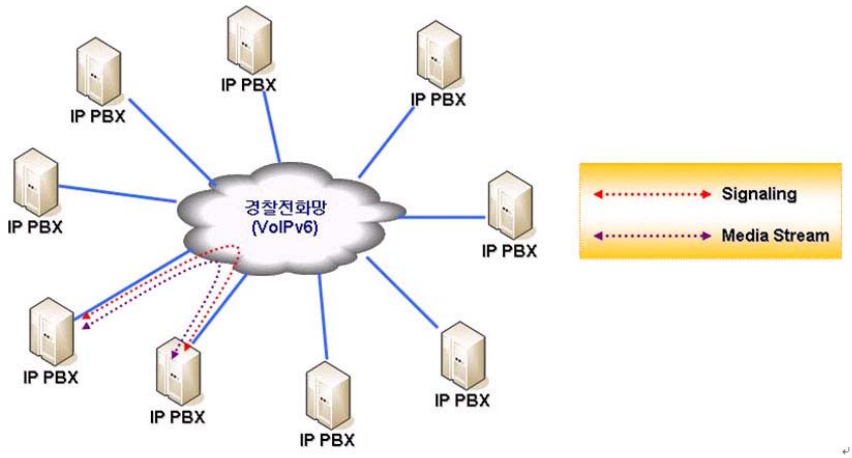
〈그림 38〉 단일기종 IPT vs. 이기종 IPT



단일 IPT 환경일 경우 위의 그림처럼 IP-PBX간 매쉬형태의 연동으로 경찰전화망을 구축할 수 있으나 이기종 IPT 환경에서는 시그널링 서버가 필요하게 된다.

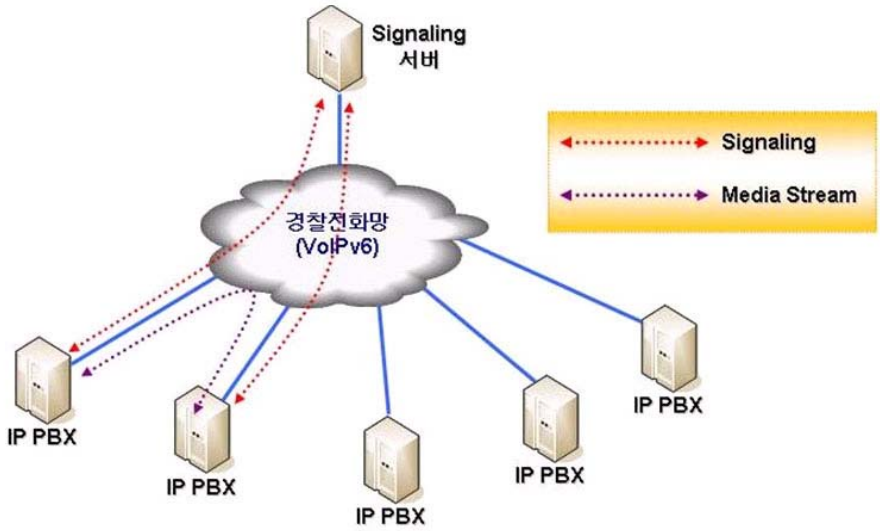
아래의 그림은 동일기종은 IP-PBX간 연동시 시그널링 및 통화 시 미디어스트림의 흐름을 나타낸다. 각각의 IP-PBX는 자체 라우팅 테이블을 통해 호의 연결대상 IP-PBX에 직접 시그널링을 보내게 된다.

〈그림 39〉 동일기종 IP-PBX간 연동



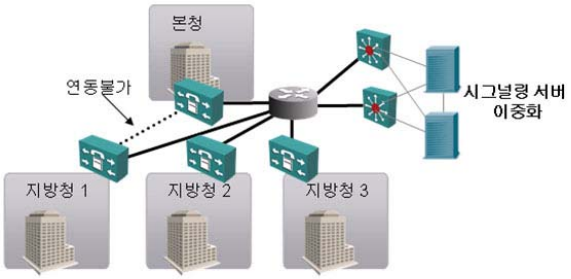
아래의 그림은 이기종 IP-PBX간 연동 시에 시그널링 및 미디어 스트리밍의 처리를 보여주는 그림이다. IP-PBX간 직접 연동이 안되기 때문에 시그널링 서버를 통해서 호가 이루어지는 형태이다.

〈그림 40〉 이기종 IP-PBX간 연동



이러한 이기종 IPT간 연동은 추가적으로 시그널링 서버의 이중화가 필요하게 된다. 아래의 그림은 시그널링 서버의 이중화를 보여주고 있다.

〈그림 41〉 이기종 IPT간 연동시 고려사항

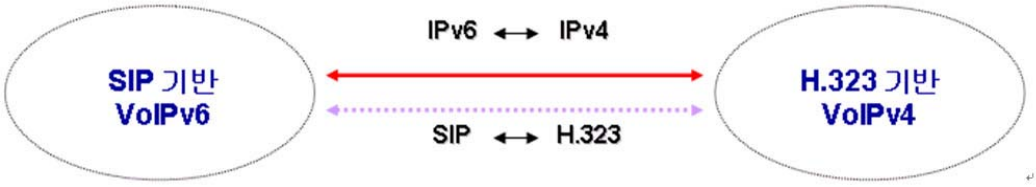


▪ 시그널링 서버를 통해서만 각각의 지방청간의 호가 라우팅 되므로 시그널링 서버 중심으로 전화번호 체계가 설계됨
- 통합관리가 되는 장점이 있지만, 동일기종 환경과 달리 추가적인 AC가 필요
- 시그널링 서버 이중화가 필요(비용부담 증가)

2. 타 망과의 연계 문제

사용자 기관 내에서 발생할 수 있는 VoIPv6와 VoIP4간 연계 및 VoIPv6와 PSTN과의 연계는 호 경로 설정에 영향을 준다. 또한 상이한 VoIP 프로토콜을 사용하는 경우 이에 대한 신호 전환을 해주어야 하기 때문에 추가적인 신호 전환 장치가 필요하게 된다.

〈그림 42〉 주소변환 및 신호전환 예



일반적으로 VoIPv6와 VoIPv4, VoIPv6와 PSTN간 연계는 인터넷전화사업자를 통하

여 이루어지나, 단계별 IPT 도입에 따라 위와 같은 연계가 발생할 수 있다. 그러나 기본적으로 한 기관 내에서 다른 인터넷 주소 및 다른 신호 프로토콜을 사용하는 것은 권장하지 않는다.

3. VoIP와 PSTN간 연동

IPT 도입에 따라 기존 PTSN과 VoIP간 연동이 필요하게 된다. 특히 기존 정부전화망과의 연동은 경찰전화망 구성에 따라 여러 가지 측면에서 고려해야 할 사항들이 존재한다.

가. 정부기관 망과의 연동

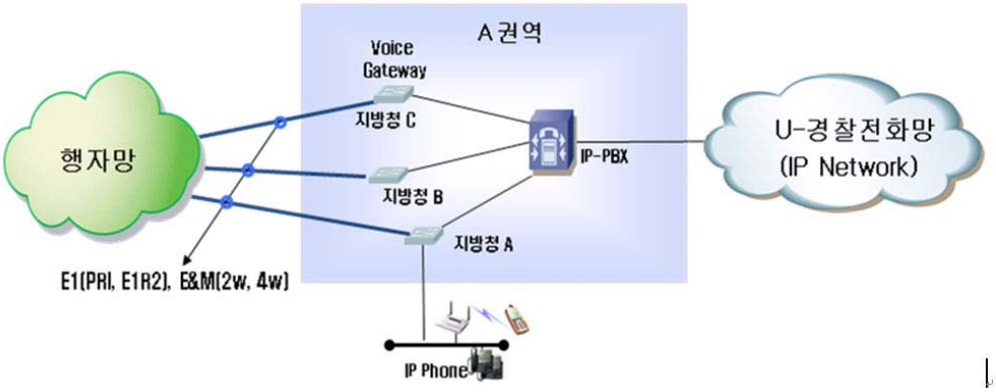
구 분	기 존	단 기	중 장 기
경찰전화망	PSTN(E1-PRI, E1-R2, E&M)	VoIP(Voice GW)	VoIP(IP-PBX or SSW)
정부전화망	PSTN(E1-PRI, E1-R2, E&M)	PSTN(PBX)	VoIP(IP-PBX or SSW)

정부기관 전화망 연동은 단기/중장기로 나누어 고려해볼 때 기존의 PSTN(PBX)기반의 VoIP-PSTN간의 연동형태를 유지하다가 정부기관망이 VoIP화 될 때 VoIP-VoIP 연동 형태가 될 것이다.

우선 정부기관 망과의 연동은 연동포인트 측면에서 고려가 이루어져야 한다. 기존의 본청 및 각각의 지방청이 정부기관망에 연동되어 있었으므로, 5개권역으로 나누었을 때 연동포인트를 5개권역의 IPT 시스템으로 할 것인지 아니면 각각의 지방청 액세스 게이트웨이로 할 것인 결정해야 하는 문제가 있다. 기존의 연동망을 그대로 유지할 경우 각 지방청에서 이를 수용할 수 있는 액세스 게이트웨이가 필요하게 된다.

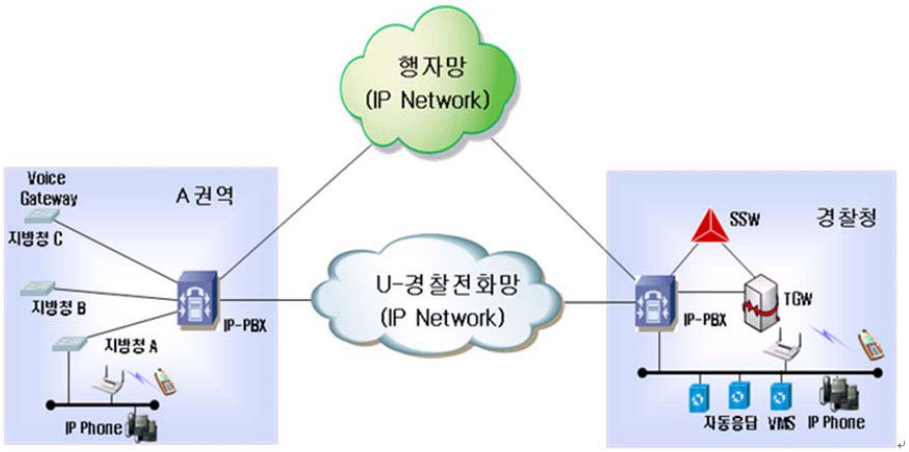
또한, VoIP 호 및 PSTN호를 동시에 처리할 수 있어야 하므로, 아래의 그림과 같이 다양한 인터페이스(E1-PRI, E1-R2, E&M,..) 지원을 위해서는 해당 인터페이스 모듈의 추가가 필요하다. 이러한 추가 모듈에 대해서는 참고자료의 Voice Gateway의 규격에 정의된 인터페이스 모듈을 기본사양으로 추가하는 것이 바람직하다.

〈그림 43〉 정부기관 망과의 연동 : PSTN



위의 그림처럼 기존의 타 기관 행정망과의 연동을 위해서는 연동장치(Voice Gateway)가 필요하다. 하지만, 이러한 다중 연동 포인트 대신 A권역의 IPT 시스템이 위치한 지방청에 단일 포인트를 둘 수도 있다. 권역 센터에 행정망과의 연동포인트를 두는 것이다. 하지만, A권역의 각각의 지방청의 연동 회선을 수용해야 하기 때문에 추가적인 PSTN 회선 증설이 필요할 수 있다.

〈그림 44〉 정부기관 망과의 연동 : All-IP



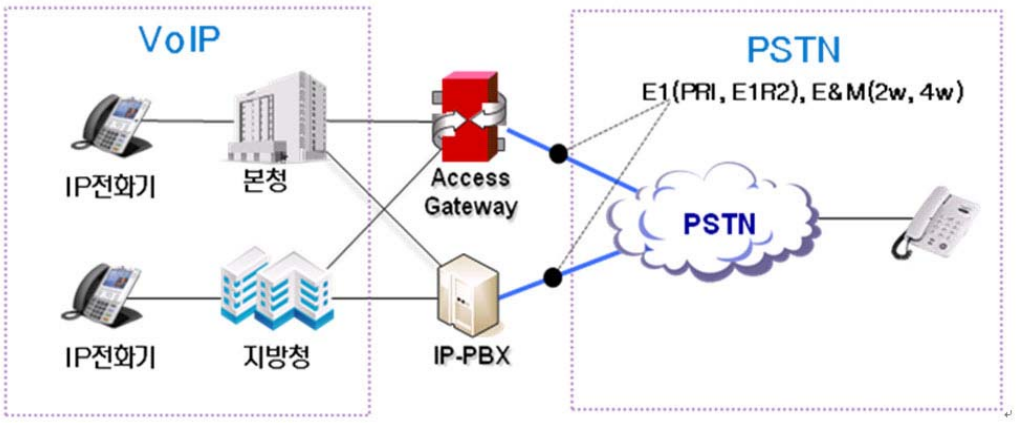
위의 그림은 차후 행정자치망이 All-IP화 됐을 때를 고려한 모델로써, 기존의 연동과는 달리 IP망을 이용한 연동이기 때문에 IP-PBX간 연동이 될 것이다. 따라서 정부의 상호 연동 규격을 따르는 장비가 도입되어야 한다.

나. PSTN(사업자망)과 경찰망간의 연동

VoIP망과 PSTN(사업자)간 연결을 경찰내에서 수행하는 경우 액세스 게이트웨이 또는 IP-PBX의 E1-PRI, E1-R2, E&M 등의 인터페이스를 연동이 필요하다. 액세스 게이트웨이 및 IP-PBX는 PSTN과 연동을 위하여 ISDN, CAS(Channel Associated Signaling) 프로토콜 등 PSTN 관련 인터페이스 표준 프로토콜을 지원해야 한다. 그리고 5개 권역으로 PSTN을 집중화했을 때 연동포인트를 권역 센터로 할 것인지, 각 지방청으로 할 것인지를 정해야 하며, 각 경찰서의 PSTN은 비상용을 제외하고는 모두 상급기관으로 통해 사용하는 것이 통신비 절감에 효율적이다.

아래의 그림은 경찰전화망(VoIP)와 사업자망(PSTN)간의 연동을 보여주는 것으로 액세스 게이트웨이 또는 IP-PBX를 통하여 PSTN과 연동된다.

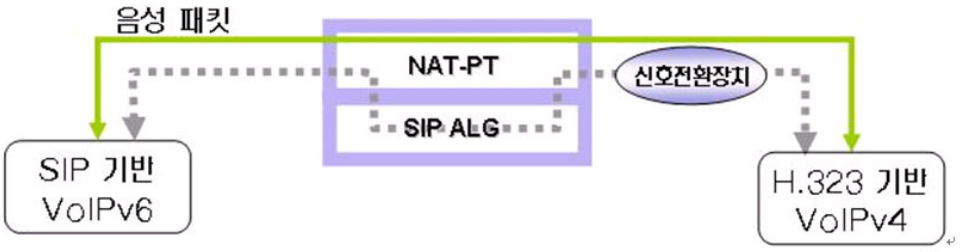
〈그림 45〉 VoIP와 PSTN(사업자) 연계



4. VoIPv6와 VoIPv4와의 연계 기술

경찰 내부와 외부 VoIP사업자간 또는 일반 사용자와의 통신을 할 때, SIP 기반 VoIPv6와 H.323 기반 VoIPv4를 동시에 사용하는 경우 신호전환장치 및 NAT-PT(Network Address Translation-Protocol Translation)를 활용한다.

〈그림 46〉 SIP 기반 VoIPv6와 H.323 기반 VoIPv4간 연계 방안



IPv4 기반 H.323 프로토콜과 IPv6 기반 SIP 프로토콜간 변환을 위하여 NAT-PT에는 SIP ALG(Application Layer Gateway) 기능이 구현되어 있어야 한다. IPv4 H.323 신호는 NAT-PT를 통하여 SIP 프로토콜 내 IP 주소 부분이 대응되는 IPv6 주소로 변환되고, IPv6 SIP 신호 또한 주소 부분이 IPv4 주소로 변환된다. 아래의 그림은 NAT-PT를 이용한 SIP 기반 VoIPv6와 IPv4간의 RTP 음성 패킷의 변환을 보여준다.

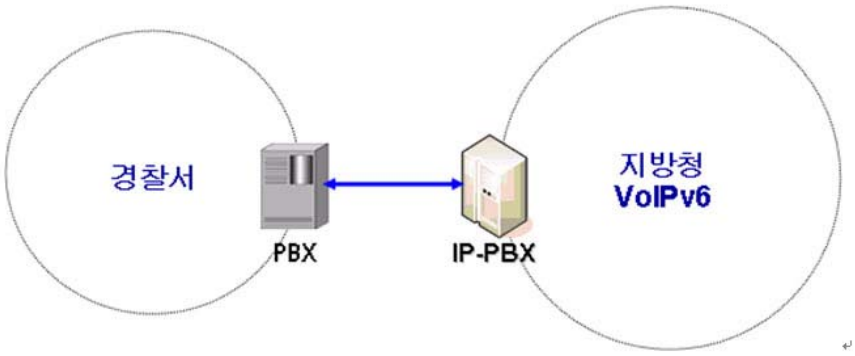
5. 기존 PBX장비와 IPT 장비간의 연동 문제

IPT 도입 초기에는 지방청 중심으로 IPT 시스템이 도입되고 이후에 각 경찰서로 확산될 것이다. 경찰서에서 보유한 기존 PBX 장비와 지방청에 도입되는 IPT 장비와의 연동 문제 및 번호체계 연계 문제가 발생된다.

이처럼 단계별 IPT 도입에 따른 기존 PBX장비와 IPT 장비간의 연동 문제는 기존의 번호체계를 유지하면서 새롭게 설계된 번호체계와 연계를 위해 VoIPv6 번호체계 설계

시 이 점을 고려하여 설계하여야 한다.

〈그림 47〉 기존 PBX와 IPT 장비간 연동 예



위의 그림에서 보듯이 경찰서 PBX와 지방청 IP-PBX간의 연동에 있어서 기존 회선인 2W E&M 연동이 필요하다. 이에 연동 가능한 IP-PBX 또는 Voice GW가 필요하다.

6. 상호 연동을 위한 규격 정의

IPT 장비간 상호 연동을 위해서는 우선적으로 상호연동에 관련된 기술 규격이 만들어져야 한다. NIA와 행정자치부에서는 공공기관에서의 상호연동을 위한 기술 규격을 제시하였다. 이와 같은 기술 규격을 토대로 경찰청 환경에 적합한 상호 연동 기술 규격이 만들어져야 한다.

이와 같이 상호 연동을 위해서는 장비 및 프로토콜, 코텍, 서비스 등에 대한 규격 정의가 필요하다. 다음은 행정자치부와 NIA의 상호 연동을 위한 각종 규격을 비교한 것이다.

〈표 21〉 프로토콜 및 음성/영상 코덱 기술 규격

구분	기능 요소		기능 설명
	NIA	행정자치부	
신호 프로토콜	SIP (IPv6)	SIP 지원	SIP 기반 네트워크의 시스템들과의 연동 프로토콜
		H.323 지원	기 구축된 H.323기반의 IPT망에서 단말들과의 연동 프로토콜
		SNMP 지원	NMS 시스템과 연동하기 위한 프로토콜
		LDAP 지원	과금/인증 서버와 연동하기 위한 프로토콜
음성코덱 기술	G.711 (필수)	G.711 (필수)	64Kbps, MOS 4.1의 우수한 품질을 제공, 대역폭 소모가 큼 (압축하지 않고 전송)
	G.729A (권장)	G.729A (필수)	8Kbps, MOS 3.7의 값을 가지고 G.711 대비 품질은 좋지 않으나 대역폭 절약 가능
	G.723.1 (권장)	-	5.3Kbps, MOS 3.65의 값을 가지고 G.711 대비 품질은 좋지 않으나 대역폭 절약 가능
	-	G.722 (권장)	G.711에 비해 품질은 좋지 않지만 대역폭 절약이 가능
영상코덱 기술	H.263 (필수)	H.263 지원	128K~2Mbps의 대역폭이 소요되는 코덱 기술
	H.264 (권장)	H.264 지원	64K~2Mbps의 대역폭이 소요되는 코덱 기술
	MPEG4 (권장)	-	128K~4Mbps의 대역폭이 소요되는 코덱 기술
음성/영상 패킷	RTP (UDP)	RTP/RTCP	SIP 표준에서 정의한 미디어 (음성,영상) 전송 프로토콜
	IPv4/IPv6 지원	IPv4/IPv6 지원	IP 주소체계에 대한 v4 및 v6 지원

〈표 22〉 음성/영상 서비스 기술 규격

구분	기능 요소		기능 설명
	NIA	행정자치부	
음성 서비스 기술	1:1 음성통화	음성통화 서비스	공공기관 내 통화, 공공기관 간 통화, 시내/시외통화, 국제통화, 착신통화 등
	다자간 통화	음성회의 통화	다자간에 음성통화 (음성 믹싱 기능, 음성 코덱 변환 기능 제공)
	방송서비스	멀티미디어 Playing	실시간 및 저장된 데이터를 단말로 지정된 포맷(코덱)으로 제공
	-	멀티미디어 Recording	동영상 정보 저장 기능 제공
	FAX 서비스	FAX 서비스	기존에 사용 중인 팩스(G3) 기능 지원 VoIP를 통하여 FAX를 전송하는 기술로 T.38 FAX Relay 권장
영상 서비스 기술	1:1 영상통화	영상회의 통화	공공기관 내, 상하위 기관 간에 영상통화로 음성전화 서비스 제공
	다자간 영상회의		1:n 형태로 공공기관 내, 상하위 기관 간에 단분할 영상을 이용한 실시간 회의 서비스 (비디오 믹싱 기능, 영상 코덱 변환 기능 제공)
	영상방송/교육서비스	-	다자간 영상회의 서비스를 응용한 실시간 및 비시실간 서비스
부가 서비스	호전환 서비스	호전환 서비스	사용자 지정한 다수의 번호 중에서 착신 가능한 번호로 호전환
	-	문서 공유 서비스	음성/영상 외의 서비스에서 문서 공유 서비스 제공
	음성사서함	IVR/MS 서비스	음성 안내 및 녹음 기능 제공
	대리응답	컬러링 (안내방송)	호대기중에 안내방송 및 컬러링 서비스 제공
	메시지 콜	클릭 투 콜	그룹전화번호부나 Call Log를 클릭하여 전화통화 서비스 제공
	-	웹모탈 기능	웹을 기반으로 한 그룹별 서비스 관리

〈표 23〉 정보보호 기술 규격

구분	기능 요소		기능 설명
	NIA	행정자치부	
정보보호 기술	신호 정보보호	-	SIP 신호 프로토콜 메시지 보호를 위해 HTTP 인증, TLS, S/MIME 등 기존 보안 기술의 재사용 권장
	음성/영상 정보보호	-	VoIP 트래픽 전달시, 인터넷 구간은 암호화 권장 (음성패킷 보호를 위해 SRTP 등의 사용 권고)
	-	트래픽 암호화	• 공중 인터넷 구간은 암호화 권장 • 신호 트래픽은 TLS 및 IPSec 기술로 암호화 권장 • 미디어 트래픽은 SRTP 기술로 암호화 권장
	VoIP와 데이터 분리	VoIP와 데이터 분리	• VLAN, 사설 IP주소 사용, ACL, F/W 등을 활용한 음성, 데이터 분리 기능 제공 • 유해 트래픽을 탐지/차단하기 위하여 응용계층 트래픽 위협여부를 판단하는 NIDS 및 패킷필터링 설정 권장
	VoIP 구성요소 보호	VoIP 장비 보호	• 단말 및 서버 시스템은 VoIP VLAN에만 연결할 것을 권장 • 허브 시스템과 같은 공유 매체는 사용하지 않을 것을 권장 • 단말 및 서버 시스템에 대한 정기적인 스파이웨어, 웜 등 취약점 정기 점검 • VoIP 서버 시스템은 본래 기능 이외의 목적으로는 활용 금지 • IP-PBX와 같은 중요 시스템은 백업 체계 유지 권고 • 중요 서버들에는 HIDS를 설치/운영하여 위협에 대비할 것을 권장
	물리적 보안	-	VoIP 서비스 제공을 위한 시스템들은 외부인의 접근을 통제하고 인증 받은 사람만 접근할 수 있도록 보안정책 수립

제2절 번호 체계 설계(안)

1. 번호체계 설계 원칙

경찰청 VoIP 번호체계 설계을 위한 기본 원칙으로, 번호체계의 최적화를 위해 다음의 번호체계 수립 원칙에 따라 설계한다.

- 전화망 또는 IPT 시스템 변경에 따른 번호체계에 미치는 영향 최소화
- 타 기관 및 지방청 등과의 단순하면서도 편리한 연계 모델 수립
- 전화번호 자릿수 최소화

시스템이나 망의 구성 변경이 있을 수 있으므로, 이러한 구조 변경으로 인한 영향을 최소화 할 수 있도록 번호를 설계한다.

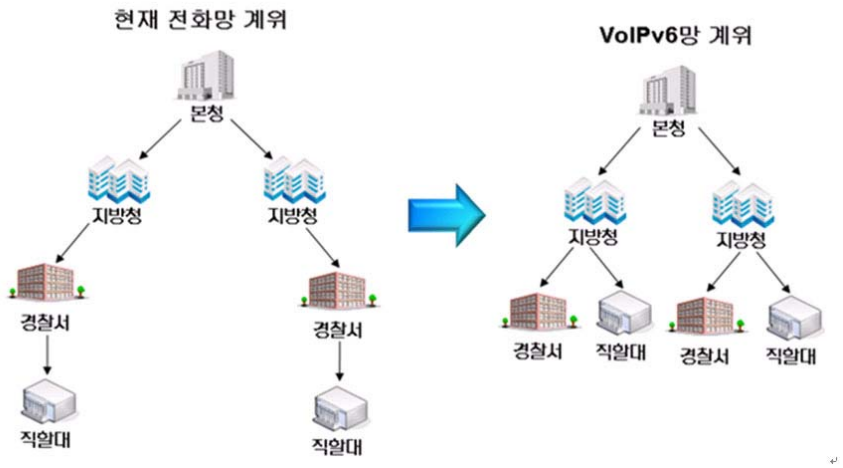
그리고 타 행정기관과 지방청간의 연동에 있어서 최소한의 액세스코드를 사용하여 단순하면서도 편리한 연계 체계 모델을 수립한다. 또한 기존 전화번호의 문제점인 10자리가 넘는 전화번호를 최소화 할 수 있도록 설계한다.

2. 번호체계 계위 변화

경찰전화망이 PSTN 중심의 망에서 IP기반 망으로 진화함에 따라 〈그림 46〉에서 보여주는 것과 같이 기존의 4단계에서 본청을 중심으로 3단계 또는 지방청 중심의 2단계 계위로 변화를 예측할 수 있다.

기존 PSTN망의 계위는 구조의 변경이 어려운 이유는 지방청에서 각급 경찰서 및 지구대를 일대일로 연결해야 하므로 충분한 회선 용량을 가지는 자체 네트워크 구축해야 하기 때문이다.

〈그림 48〉 번호체계 계위 변화



기존 PSTN망에서는 각각의 경찰서와 지방청을 지날 때마다 액세스 코드가 붙게 되지만, IPT기반 망에서는 본청과 지방청을 지나도 총 3자리 이상의 액세스코드는 붙지 않는

다. 특히 이러한 계위 변화에 따라 지방청 중심의 내선번호 구조를 가진다. 몇 개의 지방청을 하나의 권역으로 묶는 경우 IP-PBX 최대 수용 가입자에 따라 번호 설계가 달라질 수 있다. 이러한 경우 같은 권역이라도 액세스코드로 각각의 가입자를 구분할 것이다.

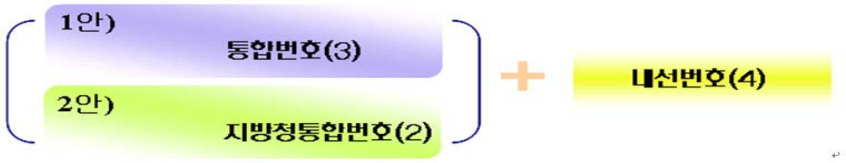
3. 번호체계 설계(안)

〈표 24〉 번호체계 설계(안)

구 분	1안(통합번호)	2안(지방청통합번호)
장 점	○ 사용자를 경찰서 단위로 식별이 가능하므로 관리 운용에 편리 ○ 단계별 음성통합 시에 유리 ○ 기존 전화번호 체계와 유사	○ 지방청 신설 시 전화 번호 부여의 용이 ○ 전화번호 자릿수 최적화
단 점	○ 경찰서 신설 시 '별도 경찰서번호' 관리 필요 ○ 전화번호 자릿수 증가	○ 전화번호의 융통성 제한 ○ 추가 Access Code 부여 가능성 ○ 경찰서 신설 시 번호 체계 관리의 어려움
검 토	이기종 IP-PBX 수용 및 6자리 전화번호로 줄이기 위해서는 2안이 적합하나, 통합 운영 및 관리측면에서는 1안이 더 적합하다.	

기존 번호체계의 문제점은 각각의 경찰서, 지방청을 경유할 때마다 추가적인 액세스코드가 붙는다는 점이다. 특히 계위가 4단계로 되어 있어서 추가적인 번호가 많아지게 된다. 이러한 번호체계를 개선하고, 이기종간 연동 및 전화망 구조를 고려하여 두 가지 개선 방안을 제시한다.

〈그림 49〉 번호체계 설계 방안



첫 번째 방안은 전국경찰을 3자리 통합번호를 부여하는 방안이다. 이 같은 통합법호 방안은 사용자를 경찰서 단위로 식별이 가능하므로 관리 및 운용에 편리하고, 단계별 음성통합 시에 유리하며, 기존 전화번호 체계와 유사하다는 장점이 있지만, 경찰서 신설 시에

별도 경찰서번호 관리 필요하다.

두 번째 방안은 전국경찰을 2자리의 지방청 중심 통합번호를 부여하는 방안이다. 전화번호를 자릿수를 최소로 할 수 있는 장점이 있으나, 경찰서 신설 시 번호체계의 일괄성 및 융통성이 떨어지고, 추가 액세스코드가 발생될 가능성이 높다. 또한, 번호체계 관리의 어려움이 따른다.

가. 통합번호(안)

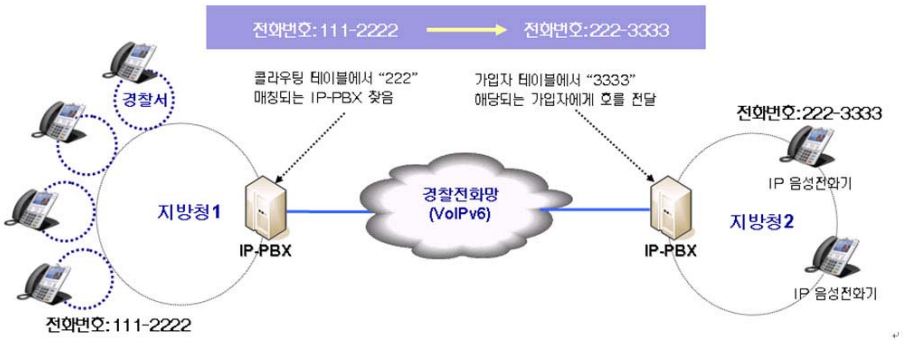
〈그림 50〉 통합번호(안)

전국경찰을 3자리 식별번호로 통합하고, 지방청 단위 IP-PBX에서 해당되는 지역의 콜라우팅(Call Routing)을 관리하는 형태이다.

각각의 경찰서, 지방청, 학교 등에 고유한 번호를 부여함으로써, 관리와 운용이 용이하며, 기존의 내선번호 체계를 유지할 수 있고, 단계 별로 음성통합에 유리하다. 하지만 각각의 IP-PBX가 관리하는 콜라우팅(Call Routing) 테이블의 증가로, IP-PBX 성능에 영향을 미칠 수 있다.

1) 통합번호(안) - 단일기종 IP-PBX일 경우

〈그림 51〉 단일기종 IP-PBX



위의 그림은 통합번호(안)의 단일 기종일 때의 통화 예로서, 지방청1 IP-PBX에 등록된 “전화번호:111-2222” 사용자가 지방청2 IP-PBX에 등록된 “전화번호:222-3333”에게 호가 라우팅 되는 과정을 보여준다.

우선 지방청1 IP-PBX에서 “222” 매핑되는 IP-PBX를 찾고, 호가 지방청2 IP-PBX에 전달되면 지방청2에서는 “3333”에 해당되는 사용자에게 호를 넘겨주는 방식이다.

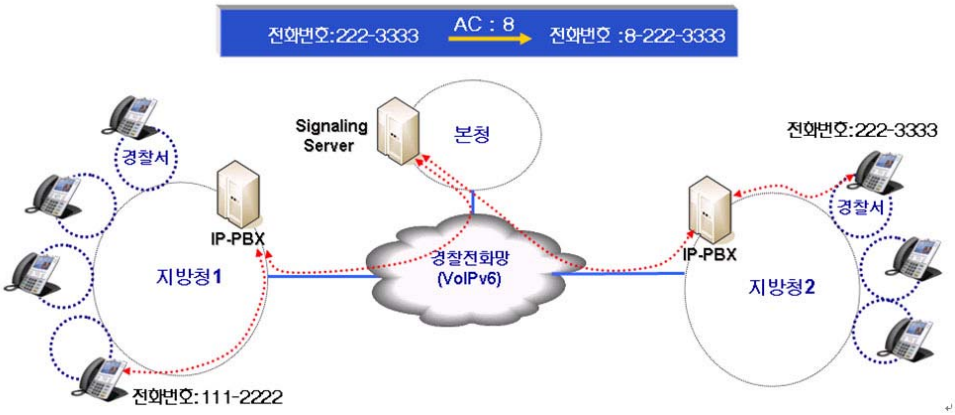
타 사업자 망 연동을 위해 내부 액세스 게이트웨이를 통한 PSTN의 연동은 “9”번을 부여하여 연동하고, 시외 지역, 이동전화 및 ITSP 사업자 망 연동을 위해 “0”으로 시작하는 번호는 외부망 연동을 위한 번호로 인식하도록 한다.

2) 통합번호(안) - 이기종 IP-PBX일 경우

〈그림 52〉 이기종 IP-PBX일 경우 번호체계

이기종 IP-PBX일 경우 IP-PBX간 연동을 위해 시그널링 서버가 필요하고, 이는 추가 액세스코드(Access Code)가 필요하다.

〈그림 53〉 이기종 IP-PBX



위의 그림은 이기종 IP-PBX 연동을 고려한 통화의 예이다.

통합번호 외에 연동을 위한 추가적인 액세스코드(Access Code)가 필요하게 되며, 모든 호는 본청의 시그널링 서버를 통해서 콜라우팅이 이루어지는 것을 보여준다. 사용자 "전화번호:111-2222"는 일단 액세스코드 "8"을 누른 후 상대방 전화번호를 누르면 본청의 시그널링 서버가 해당 IP-PBX를 찾아 호를 전달한다. 이때 지방청1의 IP-PBX에서는 "8"로 시작되는 번호가 들어오면 무조건 본청 시그널링 서버로 호를 넘긴다.

이기종 IP-PBX의 경우 타 사업자 망 연동을 위해 시외 지역의 전화번호를 누르는 경우 "8"을 누르고, 해당 지역번호를 누르는 방식을 사용하는데, 이때 시그널링 서버에서 해당 지역 지방청 IP-PBX로 호를 라우팅하고, 해당 지방청에서 시내 전화로 연결하는 방식을 사용한다.

나. 지방청 통합번호(안)

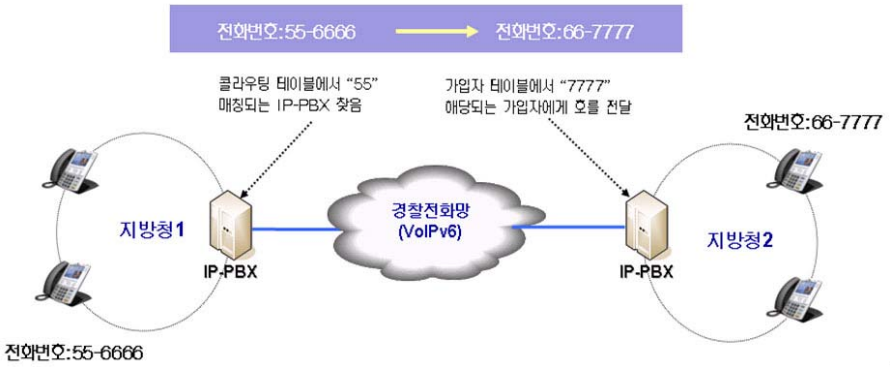
〈그림 54〉 지방청 통합번호(안)

2자리의 지방청통합번호로 전국 14개 지방청을 기준으로 전화번호체계를 설계하고, 각각의 지방청 IP-PBX가 관리할 수 있는 전화번호는 만개 미만이다. 이 방안은 지방청 예하 경찰서 및 지구대를 지방청 기준으로 번호를 할당하는 방안이다. 전화번호 자릿수를 최적화 할 수 있는 장점이 있지만, 신규 경찰서 신설 시 전화번호 부여의 어려움이 있다. 또한 향후 단말의 증가로 인한 추가 액세스 코드 부여의 가능성이 높다.

1) 지방청 통합번호(안) - 단일기종 IP-PBX일 경우

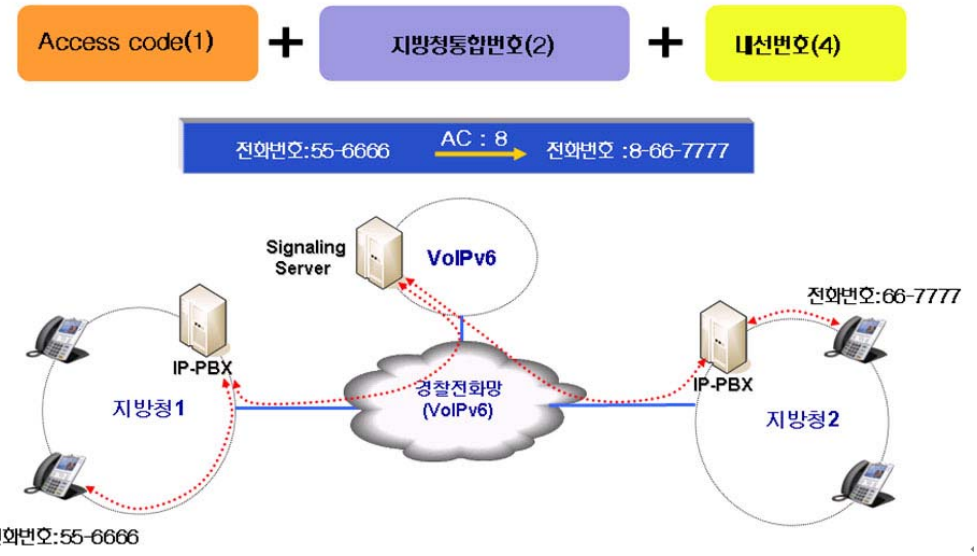
아래의 그림에서 보듯이 지방청 예하 모든 경찰서는 지방청 가입자로 등록되고, 지방청 IP-PBX에 의해 호가 라우팅 된다.

〈그림 55〉 단일기종 IP-PBX일 경우



2) 지방청 통합번호(안) - 이기종 IP-PBX일 경우

〈그림 56〉 이기종 IP-PBX일 경우



4. 내선번호 설계

내선번호 설계는 기본적으로 각 지역별 IP-PBX에 종속성을 가진다. 내선번호의 자릿수는 기존 3자리 또는 4자리를 사용하던 것을 4자리로 일괄된 형태로 적용하고, 부서별 또는 업무별, 직위별로 내선번호를 구분하여 설계 할 필요가 있다. 4자리로 적용되기 때문에 만명이 넘는 권역일 경우 액세스코드가 적용된다.

내선번호 설계는 다음의 원칙에 따른다.

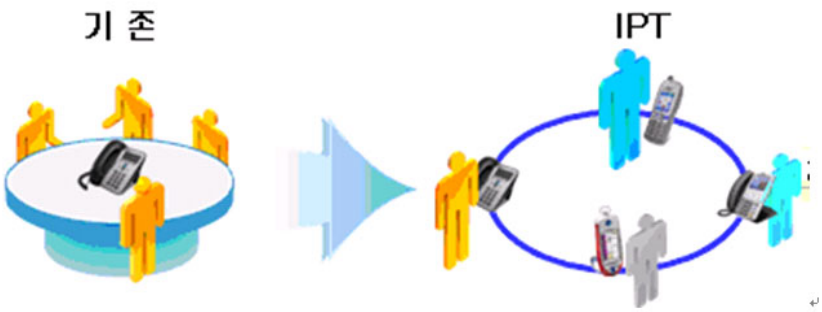
○ 1인 1번호 체계에 적합하도록 수립

○ 계층적인 번호체계 수립

○ 추가 확장 및 조직 변경/이동에 유연한 번호 체계 수립

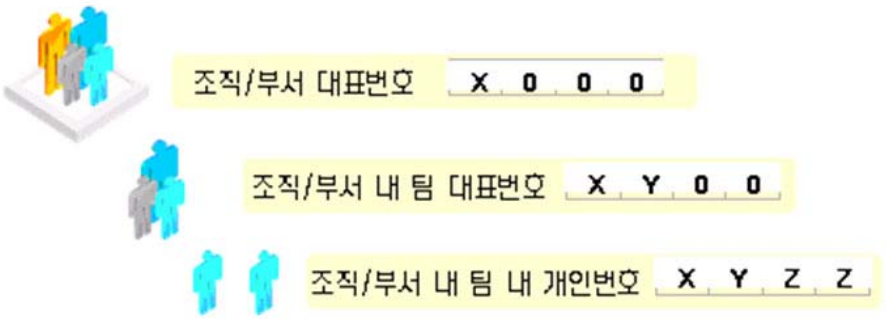
가. 1인 1번호 체계 수립

- 개개인을 구분하고 연결할 수 있는 내선번호 기반의 개인화된 번호체계 수립한다. 기존에는 내부 사용자들이 한대의 전화를 공유하던 방식에서 1인 1번호 체계로 번호를 설계한다.



나. 계층적인 번호체계 수립

- 경찰 조직 및 부서를 기준으로 한 효율적인 번호체계 정립한다.

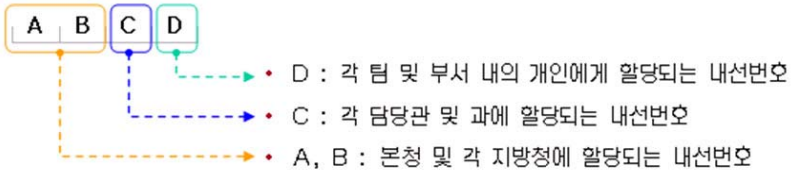


다. 추가 확장 및 조직 변경/이동에 유연한 번호 체계 수립

- IPT의 특성을 최대한 발휘할 수 있는 번호 체계 및 호 라우팅 정책 수립한다.
- 추가 확장에 적합한 형태의 내선번호 체계 수립한다.

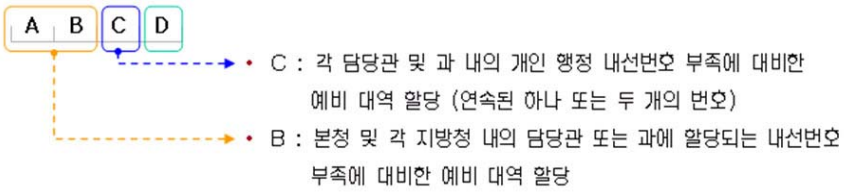
라. 내선번호 할당(안)

기본 규칙 : 내선번호 할당



각각의 범위 내에서 사용할 수 있는 대역이 부족할 경우, 상위 번호를 추가 할당하여 제공하는 형태로 확장 규칙을 따른다.

확장 규칙 : 번호 확장을 위한 예비 대역 할당

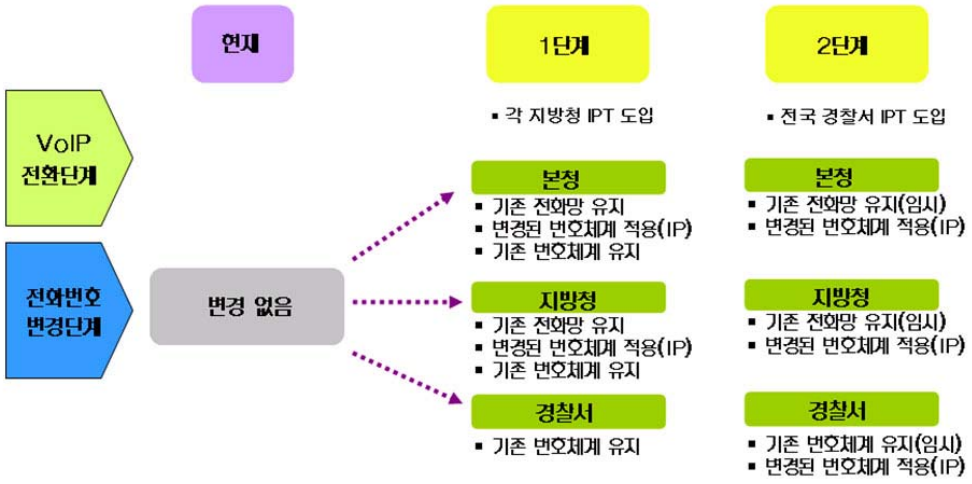


지방청 및 경찰서 수용과 향후 추가 인력 수용을 위한 예비 대역 할당을 위한 확장 규칙이다.

5. 단계별 번호체계 적용 시나리오

전국 경찰전화망에 PSTN기반망에서 IP기반망으로 변화될 때, 번호체계 적용도 이에 맞춰서 단계별로 이루어져야 한다. IPT 시스템이 단계적으로 적용된다는 가정하에 단계별 변경 시나리오를 제안한다. 다음 〈그림 55〉은 단계별 신규 번호체계 적용 시나리오를 나타낸 그림이다.

〈그림 57〉 단계별 신규 번호체계 적용 시나리오



번호체계 적용 단계는 경찰전화망의 VoIP 전환단계 즉, IPT 도입에 따라 기존의 전화번호 체계와 새롭게 적용될 번호체계가 혼용될 수 있다. VoIP전환 1단계에서는 본청 및 지방청에 IPT가 도입됨에 따라 내선번호 체계는 신규번호 체계를 도입하되, 기존 번호체계를 유지하여 병행해서 사용할 수 있도록 해야 한다. VoIP 전환 2단계에서는 안정화 기간 동안만 기존 번호체계를 임시로 유지한다.

IPT 도입 초기에는 시스템 안정화 기간이 필요하기 때문에 기존 내부 PSTN망을 유지하는 것이 바람직하다. 지방청에 IPT가 도입되었을 때 지역 경찰서와 IPT 연계(VoIP 장치)가 없으므로, 기존 망을 사용하거나, 기존망과 IPT 간의 연동을 고려해야 한다. 지방청과 경찰서 간의 회선중 일부분은 백업용으로 남겨두고, 나머지 회선은 PBX와 IP-PBX간 연동하여 새로운 번호체계를 적용하여 사용하고, 지역 경찰서에 IPT가 도입될 때, 일부 백업용 회선을 제외하고는 해지 하는 것이 바람직하다.

제6장 경찰통신망 보안

제1절 개 요

기존의 전화망(PSTN)은 지난 수십 년간 발전하면서, 매우 안정적인 서비스를 제공했고, 많은 보안문제를 해결했다. 그러나 인터넷 보급과 더불어 VoIP라는 새로운 기술이 등장하면서, 다양한 서비스 제공과 비용측면에 있어 기존의 PSTN를 앞지르고 있다. VoIP는 데이터망과의 통합과 더불어, 새로운 부가서비스 창출이 가능하게 함으로 차세대 통신서비스의 대세로 자리매김할 것에는 의문의 여지가 없다. 하지만, VoIP는 안정성과 보안성은 아직 성숙단계에 있다고 할 수 없다. VoIP는 IP의 문제점을 고스란히 가지고 있기 때문이다. 2006년에 발생한 국내 사이버침해사고 건수는 공공분야 및 민간분야 모두 전년도에 비하여 감소하였으나, 침해사고의 위험성은 증가하였다. 특히 사용자가 많은 포털 사이트의 게시판이나 자료실 등에 악성코드를 은닉하거나 전자우편에 악성코드가 삽입된 홈페이지 링크를 포함시켜 보안시스템을 회피하는 기법이 많이 사용되고 있다. 2006년 한 해 동안 발생한 국내 공공분야 및 민간분야 사이버침해사고 현황은 다음 표와 같다.

〈표 25〉 연도별 공공부문 사이버 침해사고 현황

년 도	2003	2004	2005	2006	합 계
사고현황	1,323	3,970	4,549	4286	15,850

출처 : 국가사이버안전센터

2006년에 발생한 공공분야 해킹관련 및 바이러스 사고건수는 4,286건으로 2005년 4,549건에 비하여 263건(-5.8%) 감소하였다. 사고유형별로는 악성코드 감염사고가 가장 많았으며 사고 기관별로는 지자체에서 가장 많은 사이버 침해사고가 발생하였다.

이러한, PSTN기반 망에서 IP망으로 전환함에 따른 보안 문제와 정부의 공공기관 IPv6 사업추진에 따른 IPv4망에서 IPv6망으로의 전환에서 발생되는 보안문제 그리고, IPT 도입에 따른 VoIP 보안 문제를 중심으로 다루겠다.

제2절 IP 네트워크 보안

차세대 경찰통신망의 보안은 BcN을 기반으로 하는 망에서의 보안이 될 것이다. 기존의 IP망은 단순 데이터망에서 다양한 서비스가 가능하도록 음성 및 영상, 유무선을 통합하는 BcN으로 발전해왔다. 이러한 BcN 기반으로 하는 망의 보안의 필요성과 보안 이슈 그리고, 대응방안에 대해 본 절에서 다루었다.

1. 경찰 BcN 보안의 필요성

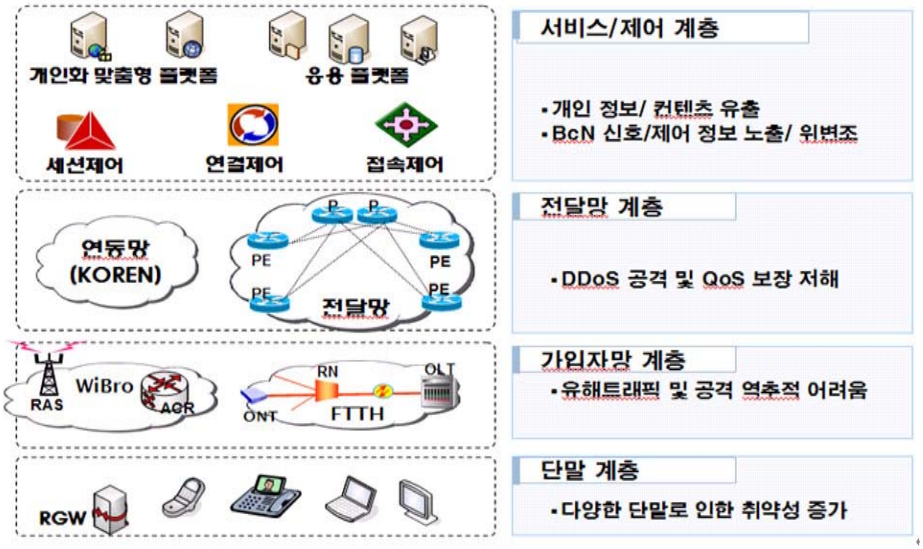
BcN의 개방형 망구조는 다양한 경로를 통하여 통신망에 대한 접근이 쉬워지고, 이를 이용한 해킹 공격 및 바이러스 유포 등의 위험성이 존재한다. BcN에서 고려되어야 할 위협요소는 다음과 같다.

- 개별 통신망에 대한 위협이 전체 통신망으로 확산될 가능성이 더욱 높아진다. 이것은 개별 통신망들이 상호 통합되기 때문에 기존의 개별적인 통신망에 대한 피해가 BcN으로 연결된 음성통신망, 방송망, USN까지 모든 구성 네트워크로 그 피해가 확산될 수 있기 때문이다. 따라서 대응 방법도 그에 따라 달라져야 한다. 현재의 네트워크 보안은 소규모 네트워크 차원에서 이루어지는 단순한 형태의 모니터링 및 보안 정책을 적용하나, BcN 환경에서는 네트워크 전체에 대하여 체계적으로 통합 관리함으로써 신속한 대응 체계를 갖출 필요가 있다.
- 네트워크 대역폭의 증가로 전송 속도가 빨라져 웜과 같은 악성 코드의 확산을 가속화 시킬 수 있다. 그러므로 네트워크 공격에 대하여 대응할 수 있는 시간도 단축된다. 이에 따라 Zero-day 공격에 대응할 수 있는 기술 개발이 요구된다.
- IPv6 기반의 BcN에서 IPv6 기능의 취약점을 이용한 새로운 공격이 발생될 가능성이 있다. 따라서 IPv4망에서 발생되었던 기존의 위협 형태를 포함하여 새롭게 IPv6에서 발생될 수 있는 취약점이 내포되고, 기존 IPv4에서 IPv6의 전환 단계에서 발생할 수 있는 위협이 있다.
- BcN과 연결된 USN에서의 취약점이 있다. 사용되는 CPU 용량이 적고 저전력을 사용하기 때문에 자원에 대한 DoS 공격에 취약하고, 분산되어 설치된 센서를 통한

개인정보보호 침해에 대한 문제가 발생할 수 있다.

이와 같이 정보통신망 기능의 마비, 개인정보의 유출, 불건전 정보의 유통 등 정보통신 환경을 저해하는 제반 위협과 부작용 등의 정보화 역기능에 대한 대응을 위하여 BcN 정보보호가 필요하다. BcN에서는 이기종 망간 통합 및 여러 사업자간에 연동이 이루어지기 때문에 체계적으로 침해사고에 대처하기 위하여 통합 정보보호 관리체계의 구축이 필요하고, 사이버 공격이 갈수록 지능화, 다양화, 고속화되는 상황에서 개별망의 피해가 다른 망으로 확산될 수 있는 환경에 대응할 수 있도록 침해사고 예방 및 대응체계에 대한 고도화가 필요하다.

〈그림 58〉 경찰 BcN 계층별 정보보호 위협



2. 경찰 BcN 보안 기술

BcN 환경에서는 다양한 콘텐츠와 서비스를 제공하는 통합망으로 설치되기 때문에 네트워크 공격의 위험성이 더욱 높아지고 취약성도 증가한다. 따라서, BcN 망에서 보안 취

약점 해결을 위한 기술로 5가지를 제시한다. (1) ESM 기반의 통합 보안 관제 센터의 구축이다. (2) 사용자 접근에 따른 접근 제어를 위하여 네트워크 접속제어 시스템과 서버 접속제어 시스템을 설치한다. (3) 서버 보안 및 컨텐츠 보호를 위한 CAS를 도입하고, 침입 탐지를 위한 IDS 장비를 구축한다. (4) 네트워크 보안을 위하여 비정상 트래픽 감지/분석/제어를 위한 장비가 필요하고, 싱크홀, 블랙홀 라우터를 구축과 침입방지시스템을 구축한다. (5) 고객 단말 보호를 위하여 고객 PC에 유해 패킷 차단 시스템을 설치하여 보호한다.

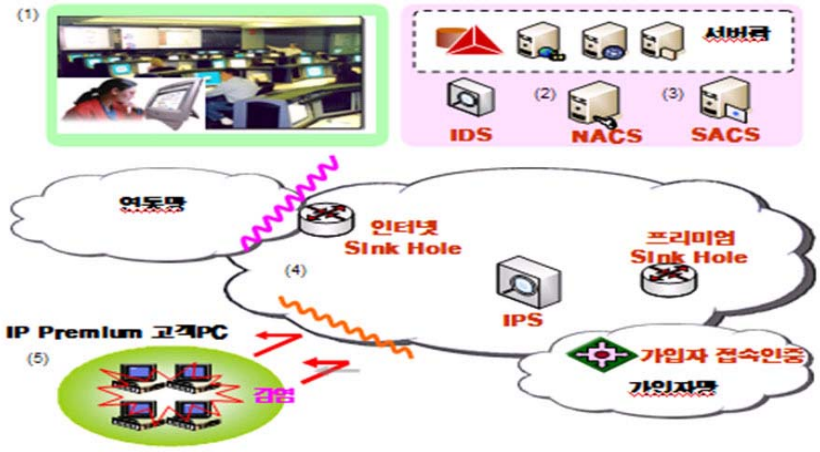
방화벽, 침입탐지시스템(IDS), 가상시설망(VPN) 등 네트워크를 통해 들어오는 모든 위험요소들을 총체적으로 분석하여 미리 사전에 예방할 수 있도록 운영자에게 알려주는 시스템이다. 네트워크 운영자 및 서버시스템 운영자는 ESM을 통하여 얻어온 위험 정보를 바탕으로 네트워크에 생겨질 이상부분을 미리 파악하고 대처할 준비를 함으로 시스템 운용을 원활하게 할 수 있다.

웹 서비스, 전자메일, P2P 인스턴트 메시지 등과 같은 다양한 서비스 정보에 유해 및 불법 정보를 많이 포함하고 있는 Phishing 및 Pharming, 스팸, 악성코드, 사회공학 등의 공격이 증가하고 있다. 이런 공격에 대응하기 위하여 콘텐츠 기반 보안 기술로 침입 탐지기술이 개발되었다. 침입 탐지장치는 외부에서 침입하는 악의적인 공격에 대하여 콘텐츠 보호 및 데이터를 보호한다.

외부에서 유입되는 공격을 사전에 봉쇄하기 위하여 네트워크 망에는 침입 방지 장치가 필요하다. 침입 방지 장치는 알려진 공격기법이나 의심되는 데이터를 분석하여 네트워크 망에 유입되는 공격 데이터를 사전에 차단한다.

BcN 환경에 접속하는 단말은 다양한 이기종 망에서 접속되기 때문에 각 망의 취약점에 그대로 노출된다. 이러한 취약점을 사전에 방어하기 위하여 사용자 단말은 유해 패킷 차단을 위한 백신이나, 개인 방화벽과 같은 S/W 기반의 보안장비를 설치하여 데이터를 보호한다.

〈그림 59〉 경찰 BcN 보안 기술



3. 경찰통신망 보안서비스 방안 설계(안)

인터넷 기술의 발전과 함께 악의적인 공격은 다양한 형태로 변경되어 사이버 세상을 위협 하고 있다. 이러한 환경에서 경찰망의 All-IP화는 BcN의 위협에 노출되기 때문에 보안 강화를 위한 새로운 보안구조가 필요하다.

본 절에서는 경찰망 고도화에 따른 보안위협을 사전에 보호하기 위하여 3가지 관점에서 보안서비스 방법을 제안한다. 첫번째, 단말의 데이터 보호를 위한 다단계 보안서비스 제공 방법과 두번째, 외부에서 침입하는 공격의 탐지 및 차단을 위한 방법 마지막으로 보안장비의 통합관리를 위한 관리 방법을 제안한다.

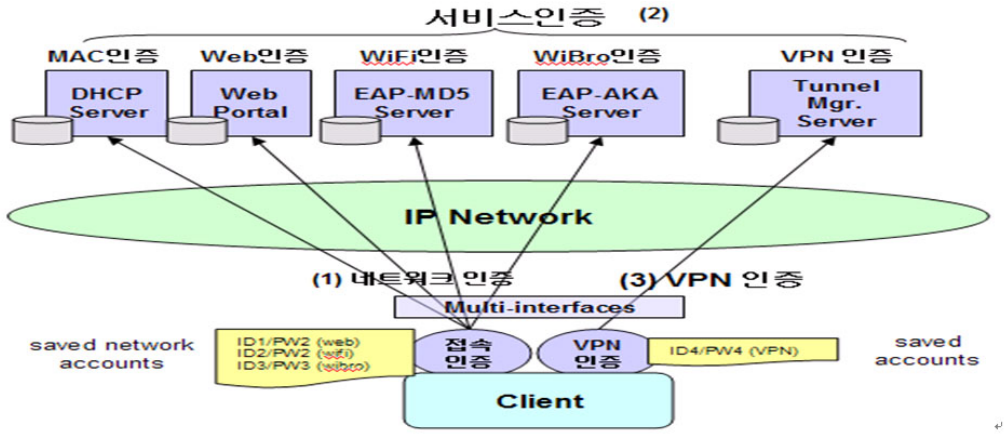
가. 다단계 보안 서비스

경찰 통신망 고도화에 따른 다단계 보안 체계는 크게 3가지 관점에서 접근한다. 첫째, 단말의 보안 서비스 제공을 위한 통합 인증, 두번째, 단말 통신의 데이터 보호를 위한 데이터 암호화, 마지막으로 All-IP화에 따라 서비스 분리를 위한 가상 사설망 생성 방안이다.

1) 통합 인증

경찰 통신망의 통합 인증방법은 네트워크인증, 각 응용 서비스 제공을 위한 서비스인증, 단말의 데이터 암호화를 위한 VPN인증으로구분한다. 첫번째, 네트워크 인증은 외부 네트워크와 통신을 위한 AAA 서버 기반의 인증 서비스 제공을 위하여 ID/PW기반의 외부 인증서버와 연동이 필요하고, 이를 기반으로 통합 접속 인증방안이 필요하다. 두번째, 서비스 인증의 경우 사용자 권한에 따라 일반, 품질, 보안/품질 등급으로 구분하고, 보안이 적용될 경우 인증서 기반의 서비스 접근 통제가 필요하다. 세번째, VPN 인증은 PKI 인증서를 기반으로 접속통제를 수행하고, IPSec 기반의 데이터 암호 전송이 필요하다.

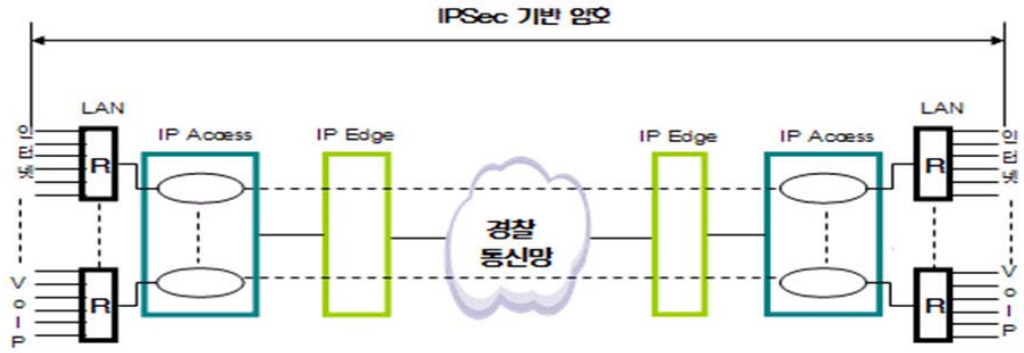
〈그림 60〉 통합 인증 체계



2) 데이터 암호화

경찰 통신망의 안전한 데이터 통신을 위하여 경찰망 전구간의 단대단 데이터 암호화 서비스 제공 방안이 필요하다. 현재 단대단 데이터 암호화를 위하여 IETF에서 PKI 기반의 IPSec을 연구가 진행되었고, 2007년 8월에 표준화가 완료되었다.

〈그림 61〉 데이터 암호화 구조



이러한 IPsec은 OSI 모델의 네트워크 계층(layer 3)에 존재하며 보다 안전한 네트워크 기반 서비스 지원을 위한 목적으로 표준 IP를 확장함으로써 본래의 IP 주소를 숨겨 네트워크 침해로부터 데이터를 보호하는 기술이다. IPsec은 암호화, 인증 및 키 관리등 강력한 보안 기능을 탑재하고 있기 때문에 IP 환경에 있어 최고의 터널링 프로토콜로 받아들여지고 있으며 다음과 같은 특성을 가지고 있다.

□ 데이터 기밀성 보장

- 3DES/AES 등의 암호화 알고리즘을 통한 데이터 암호화로 지정된 사용자만 데이터를 확인할 수 있다.

□ 데이터 무결성(Integrity) 보장

- MD5, SHA-1 등의 Hash 기법을 통한 checksum 적용으로 허가된 사람들에게만 데이터가 수정될 수 있음을 보장한다.

□ 데이터 근원지에 대한 인증

- IP 데이터그램에 비밀 공유키(Secret Shared Key)를 삽입하여 활용한다.

□ 재전송(Replay) 공격 방지

- Sequence Number 관리를 통해 타인이 중요 메시지를 가로채어 똑같은 메시지를

전송하는 공격을 방지한다.

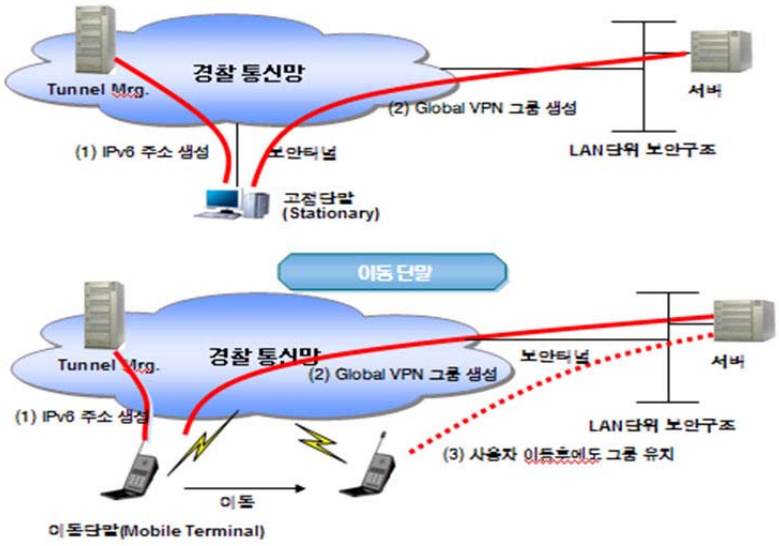
3) 가상 사설망 생성

경찰 통신망의 All IP를 고려하여 3가지 VPN 기능이 필요하다. 첫째, 단말과 서버간의 Global VPN, 둘째, 서버와 서버간의 네트워크 VPN, 마지막으로 단말 그룹을 생성하는 CUG VPN 적용 방안이다.

◎ Global VPN

단말의 위치에 상관없이 특정 그룹을 생성해주는 기술인 Global VPN 서비스 제공을 위하여 고정 및 (1) 이동 노드에 위치한 단말은 Tunnel Manager에 접속하여 IPv6 주소를 생성하고, 생성된 IPv6 주소를 기반으로 위치 독립적인 노드 그룹의 생성이 필요하다. 생성된 IPv6 주소는 터널 관리 서버에 접속하여 소속된 위치정보를 기반으로 생성되며, Prefix 정보를 기반으로 그룹을 생성한다. 만약 사용자가 이동할 경우 이동 단말의 IPv4 주소는 변경되지만, IPv6주소는 유지되기 때문에 서버에 재접속하여 이동전의 사용자 그룹은 유지되어야 한다.

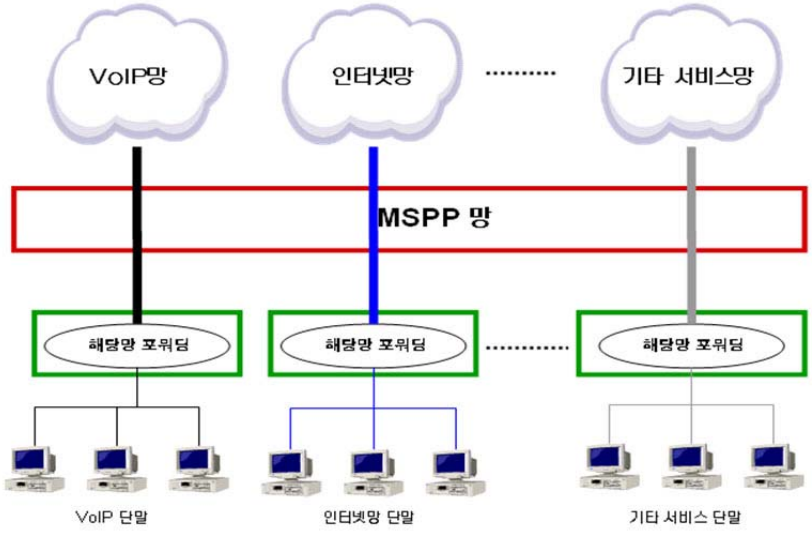
〈그림 62〉 Global VPN



◎ Network VPN

Network VPN은 All IP화 되는 경찰 통신망의 서비스를 구분하여 Quality 및 Security이 보장된 인프라를 기반으로 망을 구분하는 서비스를 제공한다. 〈그림 63〉과 같이 모든 망의 통합에 따라 망 구성을 위한 트래픽을 물리적으로 완벽히 분리가 필요하다.

〈그림 63〉 Network VPN



◎ CUG VPN

P2P CUG 구성을 위하여 P2P Management System에 접속하여 IPv6 기반의 주소와 피어 정보를 받아오고, 이를 기반으로 QoS 및 보안서비스를 정의한다. 정의된 서비스는 각 사용자에 따라 그룹을 생성하고, 그룹에 소속된 사용자들의 통신 서비스가 필요하다.

나. 침입 탐지 및 차단 시스템

최근 상용망에서 지속적으로 보고되는 네트워크 공격들을 살펴보면 바이러스, 웜, 트로

이 목마, 악성 코드의 특성을 모두 갖고 있는 혼합 보안 위협(Blended Threat)이 대부분이다. 공격을 시작, 전파, 확산시키기 위해 서버와 네트워크의 취약점을 이용하는 혼합 보안 위협은 그 피해 사례가 매년 2배 이상 급증할 정도로 심각한 수준에 이르렀다. 경찰 통신망은 상용망과 분리된 망이지만 그러한 네트워크 공격에 안전하다고 볼 수 없다.

현재 방화벽, IDS, IPS 등의 장비에 따라 네트워크 망의 위협을 탐지 및 방지하고 있으나, 1.25 사태 발생 원인과 같이 기존 네트워크 보안장비는 패치가 배포되기 전의 공격방법인 Zero-Day 공격에 대한 대응이 어렵다. 따라서, 내부 네트워크 이상징후 발생 시 사용자 체감 이전에 조기 예/경보기능 지원과 위협상황 발생에 대한 라이프사이클 관리, 차후 위협 발생 시 적절한 의사 결정수단 지원을 위한 네트워크 분석 및 대응체계 지원이 필요하다.

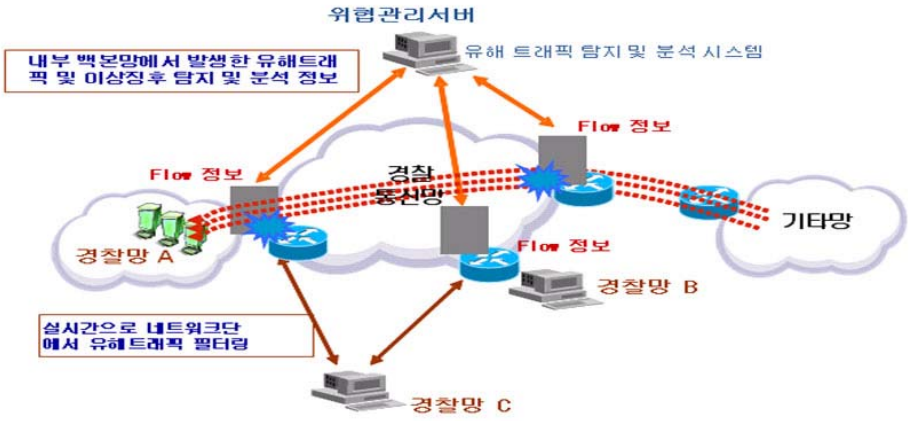
◎ Flow 탐색 시스템

통신망 사용자 증가와 다양한 응용 발전에 따라 트래픽은 급속도로 증가하고 있으며, 이와 더불어 다양한 공격기술들이 등장한다. 통신망트래픽의효과적인관리및비정상트래픽에대한공격사전탐색을위한 Flow 탐색 및 분석 시스템 필요하다. 트래픽의 효과적 관리 및 비정상 트래픽 탐색을 위하여 IP Edge level에서 Flow 정보를 탐색하고 위협 탐지 시스템에 수집된 Flow 정보를 포워딩 해야 된다. 또한 세션별 사용량 정보를 수집 및 보관하여 트래픽을 분석하고, 노드/모듈별 트래픽 상태를 분석하여 이상 트래픽 감지를 위한 기능이 필요하다.

◎ 위협관리 시스템

대규모 네트워크를 운영하는 경찰망에서 로컬과 글로벌 트래픽 이벤트에 대한 종합적인 분석을 수행하여 웜, 해킹, 사이버테러, 비정상 이상행위 등의 공격을 예보, 경보를 위한 시스템이 필요하다.

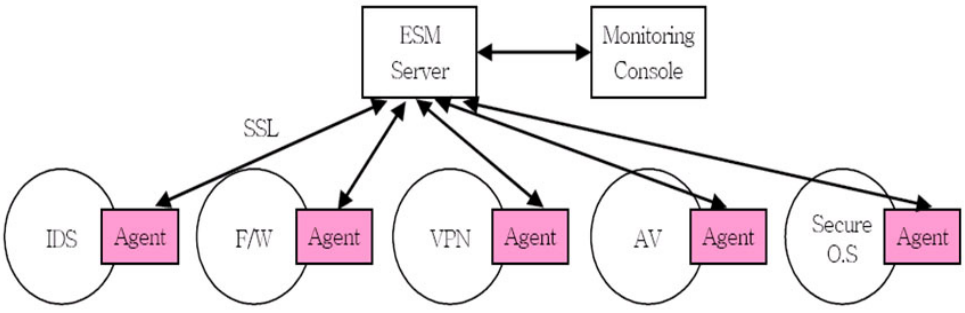
〈그림 64〉 위협관리 시스템



◎ 통합관리시스템

통합관리시스템은 관리 대상 장비(침입차단, 침입탐지, 가상사설망, 안티바이러스 등)와 여기서 발생하는 정보를 수집하는 중앙관리시스템, 그리고 관리자가 활용할 수 있는 인터페이스를 제공하는 콘솔, 정보 수집을 위하여 관리 대상 장비에 설치되는 에이전트로 구성된다. 서버와 에이전트와의 통신을 통해 상태 정보가 수집되면 수집된 정보는 콘솔에 표현되고, 통신되는 데이터의 안전성을 보장하기 위해 양방 간의 통신은 보안 알고리즘을 사용할 수 있다. 통합관리시스템은 〈그림 65〉와 같이 구성된다.

〈그림 65〉 통합관리시스템 전체 구조



- 통합관리시스템 구성 요소

  통합보안관제체계의 구성요소는 크게 에이젼트와 보안관제체계 서버와 콘솔이 있다. 에이젼트는 각 정보보호 시스템에 탑재되며, 보안관제체계 서버와 콘솔은 지역보안관제시스템 및 통합보안관제시스템을 구성하는 구성요소이다. 에이젼트는 정보를 수집하여 서버로 전송하는 기능을 수행하고, 보안관제체계 서버는 에이젼트로 부터 수집된 이벤트/로그를 수신하여 분석하고, 콘솔의 그래픽 사용자 인터페이스를 통해 각종 운영 정보를 표시하거나 실시간 경보를 수행하게 된다.

- 에이젼트

  정보보호 시스템에 구현되는 구성요소로써 경찰망에서는 VPN 게이트웨이와 통합보안장비에 에이젼트가 탑재되게 된다. 에이젼트는 정보보호 시스템에서 발생하는 로그와 이벤트를 수집한다. 수집된 로그와 이벤트는 보안관제체계 서버와의 메시지 전송방식을 통해 서버로 전송된다. 또한, 서버에서 전송된 메시지를 통해 정보보호 시스템의 구성설정 변경 및 검색, 보안정책의 설정, 변경 기능 등을 수행하게 된다.

- 통합보안관제 서버

  통합보안관제시스템과 지역보안관제시스템에 위치하는 구성요소이다. 통합보안관제서버는 에이젼트로부터 이벤트/로그 정보를 수신하고 콘솔에 각종 보고 및 경보 전송, 콘솔 요청 정보 제공하고, 콘솔 명령을 수행하거나 에이젼트로 전송한다.

  통합보안관제서버의 기능들을 크게 구성관리, 바이러스 관리, 이벤트 모니터링 및 분석 기능, 위험관리, 취약점 분석, 리포트 및 검색 기능, 보안정책 관리 등을 수행한다. 기능에 대해 자세히 살펴보면 다음과 같다. 이들 기능 중에 위험관리 및 취약점 분석기능은 주/부 통제국에 위치한 통합보안관제시스템을 구성하는 서버에만 제공되는 기능이다.

- 콘솔

  콘솔은 웹 기반의 그래픽 사용자 인터페이스를 제공하여 관리자에게 실시간 경보 및 정보 제공을 수행하는 구성요소로써, 관제기능과 운영기능 및 보안관리기능 등을 지

원한다. 먼저, 관제 기능을 통해 실시간 종합관제, 실시간 경보, 추적, 대응을 위해 관제 상황을 화면에 표시하여 관리자가 모니터링 할 수 있으며 지도표시 기능을 가지게 된다. 운영기능을 통해 상태 모니터링과 장애 이력 조회, 장애조건, 경보 기준 설정 및 구성정보 조회 및 설정 편집 기능을 수행하고 보안 정책을 조회하고 편집하는 기능을 수행하게 된다. 또한 유형별 생성된 리포트를 해당 포맷으로 화면에 표시하고 출력하는 기능을 제공한다.

- 운용구조

  종합분석대응체계가 구축된 통합보안관제체계는 지역분산 운용구조를 가지게 된다. 주/부 통제국의 통합보안관제시스템에서는 차세대 경찰전화통신망 전체의 정보보호 시스템 관리 및 위험관리, 취약점 분석기능을 수행하지만, 지역통제국 내의 지역보안관제시스템에서는 각 지역의 정보보호 시스템에 대한 관리 및 제어를 수행하게 되며, 각 장비에 탑재되어 있는 통합보안관제체계 에이전트를 통해 이벤트 및 로그를 수집하는 기능을 수행하게 된다. 또한, 정보보호 시스템의 구성 및 상태 정보를 관리하고, 제어하는 기능 및 정보보호 시스템에 대한 정책관리 기능 등을 수행하게 된다.

제3절 VoIP 보안

VoIP 기술은 기존 IP기술을 이용하여 음성 통신 서비스를 제공하기 때문에 IP 기반의 위협들을 그대로 상속하며, VoIP 서비스 제공을 위한 신규 기술들로 인해 발생하는 새로운 위협들을 가지고 있다. 그 중에서도 공격 가능성 및 피해 규모 등을 고려할 때, 도청, 서비스 거부공격, 서비스 오용공격, 세션 가로채기, 스팸 공격 등은 가장 문제가 될 수 있는 보안 위협이다.

- 도청 : 사용자의 통화 내용을 공격자가 청취할 수 있다.
- 서비스 거부 공격 : 주요 VoIP 서비스 관련 시스템 또는 단말에 대한 공격을 통해 정상적인 서비스 제공을 방해한다.

- 서비스 오용공격 : 인가 받지 않는 사용자가 불법으로 인터넷 전화를 사용하여 과금을 회피하는 공격이다.
- 세션 가로채기 : SIP 프로토콜의 사용으로 대두된 새로운 위협으로써, 호 설정 과정에 개입하여 사용자의 세션제어권한 등을 획득하는 공격이며 도청, 서비스 오용 등 2차 공격을 유발할 수 있다.
- VoIP 스팸 : 자동화된 도구를 사용하여 불특정 다수에게 다량의 광고성 음성 또는 문구를 전송하는 공격을 의미하며 기존의 스팸과 비교하여 VoIP 스팸은 저렴한 비용 및 대량 발송의 편의성으로 커다란 사회 문제로 대두될 것으로 예상된다.

〈표 26〉 VoIP 정보보호 위협

보 안 위 협		
대분류	중 분 류	세 부 분 류
도 청	LAN 구간에 대한 도청	회선공유 트래픽 도청
		ARP Cache Poisoning
		IP-PBX 해킹을 통한 도청
		원격 PC 해킹을 통한 도청
	WAN 구간에 대한 도청	SIP Proxy 해킹을 통한 도청
		Registrar 해킹을 통한 도청
		라우터 및 네트워크 시스템 해킹을 통한 도청
	단말도청	웜, 바이러스 등을 통하여 권한 획득 후, 원격제어
		도청 악성코드 삽입
		단말기 패스워드 취약점 공격(사용자, 관리자)
서비스 거부공격	시스템 자원고갈	SIP Invite flooding
		RTP flooding
		UDP, ICMP, Echo 등 flooding
	회선자원고갈	DDoS 공격
	통화방해 및 중단	SIP-Cancel DoS 공격
		RTP-SSRC Collision 공격
		RTCP Insertion 공격
		SIP-Bye 공격
		DHCP 서버 삽입공격
	해킹을 통한 시스템 장애	소프트스위치, SIP Proxy 해킹
		SIP Registrar 해킹
		게이트웨이 해킹
		GateKeeper 해킹

서비스 오용공격	등록정보 변조	Contact 정보를 공격자의 IP 주소로 등록
		Contact 정보에 공격자의 IP 주소 추가 (Forking)
		SIP SQL Injection 공격
	관리상의 오류공격	Gatekeeper
		SIP Proxy(SSW)
		SBC
		단말기 패스워드 취약점 이용하여 단말 복제
	시스템 해킹을 통한 설정 변경	소프트스위치, SIP Proxy 해킹
		SIP Registrar 해킹
		게이트웨이 해킹
		GateKeeper 해킹
세션가로채기	Invite 세션 가로채기	프락시 서버 가상 MITM 공격(도청, 통화중단)
	SIP Registration 하이잭킹	공격자 IP로 등록(서비스 오용가능)
VoIP 스팸	Call 스팸	음성 스팸
	IM 스팸	인스턴트 메시스 스팸
	Presence 스팸	프레즌스 정보를 이용한 스팸
	비싱	사회공학적 방법을 통한 개인정보 취득(금융사고 발생)

1. VoIP 보안 위협 대책

가. 안전한 네트워크 및 시스템 구축

VoIP 서비스 환경의 보안 위협을 최소화 할 수 있도록 안전한 네트워크 및 시스템을 구축하고, 접근을 제어 등의 보호 대책을 조치한다.

- 안전한 네트워크 구축 : 사설 IP 망으로 구축하여 내부 VoIP 단말 및 시스템들에 대한 구성 정보를 외부에 노출 시키지 않는 기법을 적용한다.
- VoIP 장비 접근제어 : VoIP 단말에 대한 악의적 공격자의 접근을 차단할 수 있는 접근제어 기술을 적용한다.

나. 침입대응 및 모니터링

안전한 VoIP 서비스 보호를 위해 웜•바이러스 등의 악성코드 대응 및 유해 트래픽 차단 등 악의적인 공격을 사전에 탐지하여 차단해야 하며, 장애가 발생하더라도 VoIP 서비스의 지속적인 제공이 가능하도록 해야한다.

- VoIP 장비에 대한 악성코트 탐지 및 보안 점검
- 백도어 및 해킹을 위한 에이전트가 설치되어 있는지 여부와 불필요한 서비스가 활성화 되어있는지 등을 점검해야 한다.
- 이상 징후 발생 정보와 관리자 및 사용자 접근에 대한 로그를 남기고, 주기적으로 점검해야 한다.

다. 사용자 인증

VoIP 서비스 사용자의 신원확인 및 접근제한 정책을 마련하고, 권한 있는 사용자만 해당 서비스를 사용하도록 필요한 조치를 취하여야 한다.

- 사용자 인증 : 정당한 사용자 인지의 검증 및 인증 메커니즘 적용
- 관리자 인증 : 네트워크 및 VoIP 장비에 대해여 정당한 관리자인지 검증하기 위한 관리자 인증 메커니즘을 적용

라. 제어 및 미디어 신호 등 트래픽 보호

사용자의 제어 및 미디어 신호에 대하여 권한 없는 제3자에 의한 수집 및 이용을 방지하도록 조치를 취하여야 한다. 다만 조치를 취하지 못할 경우에는 이용자에게 약관 등을 통한 보안 위협에 노출 될 수 있음을 사전에 고지하여야 한다.

- VoIP 트래픽 암호화 통신 : 호설정 관련 데이터를 보호하기 위해 제어 신호를 암호화 하여야 한다.

〈표 27〉 SIP 정보보호 기술

구 분	기술 설명	보안기능
HTTP 인증	HTTP에서 사용되는 인증방법으로 Digest 인증만을 사용하며, 재사용 공격방지의 인증기능을 제공함(RFC2617)	사용자 인증
TLS (Transport Layer Security)	SIP 메시지에 대한 암/복호화를 통하여 홉간 신뢰구간을 형성하여 SIP 메시지의 기밀성과 무결성을 제공함 SIP 서버에서는 TLS 기능을 반드시 지원해야 하며, SIP 단말에서도 TLS 지원을 권고함	홉간 보안
S/MIME (Secure/Multipurpose Internet Mail)	종단간 SIP 사용자에게 보안기능을 제공하고, 메시지에 대한 기밀성, 무결성과 상호 인증 기능을 제공함(RFC 2633, RFC3261)	양단간 보안

- VoIP 관련 장비 관리 트래픽 암호화 통신 : 단말을 관리하기 위한 관리 메시지 전송 시 암호화 하여 통신한다.

2. IPT 보안

인터넷전화 서비스는 인터넷 기반의 기술을 사용하므로 인터넷망에서 발생하는 보안 위험성이 내재되어 있고, 실시간 서비스 특성으로 기존 보안 솔루션의 수정이나 변경 없이 보호하기는 어려운 면이 있다. 따라서 인터넷전화를 구축하는데 있어서 요구되는 보안성에 대한 세부지침을 수립하여 일관성 있는 보안 요구사항의 적용이 필요하다.

가. IPT 보안의 목표

- 인터넷전화의 보안성은 다음의 내용을 목표로 수립되어야 한다.

〈표 28〉 IPT 보안의 목표

구 분	주 요 내 용	비 고
기 밀 성	데이터 및 정보가 정당하게 인정되는 단말, 시스템 및 프로세스에만 개방시키는 것으로서, 통신정보의 암호화를 통하여 정보를 보호	정보누출의 방지
무 결 성	통신 정보의 위/변조를 방지하여 데이터 및 정보가 정확하고 완전하여 오동작을 방지.	정보의 변조 및 파괴를 예방하고 방지
가 용 성	외부의 공격에 대해서 시스템의 안정적인 동작을 보장 시스템에 요구된 방법으로 적시에 접속과 이용이 가능	해킹으로 인한 시스템 동작 불능 예방
접근제어	선택된 기기 및 이용자에 대한 시스템 접근 허용.	정보접근의 물리적 보안
인 증	통신서비스를 사용하고자 하는 기기 및 이용자에 대한 신원 확인	정당한 사용자의 확인

나. 보안 요구사항

인터넷전화에서 정보보호 요구사항은 VoIP 프로토콜의 보안 특성과 IP 기반 환경에서 현재 알려진 취약점 및 잠재적인 보안위협 유형을 이해하여 인터넷전화 구축 및 서비스제공에 앞서 고려해야 하는 정보보호 목표라고 할 수 있다. 따라서 안전한망 설계 방안과 장비 및 트래픽 보호, 접근통제, IP 보안 위협에 대한 대책 등이 강구 되어야 한다.

〈표 29〉 보안 요구사항

정보 보호 요구 사항	주요 내용	비 고
안전한 망설계	인터넷전화 IPT로 별도 구축	
장비보호	서버 보호 단말 보호	
트래픽 보호	Signaling 트래픽 제어 및 인증(Diget 인증) Signaling 트래픽 암호화 (SRTP) Media 트래픽 암호화 (TLS)	표준기술채택
접근통제	방화벽/NAT 통과 기능	
IP보안위협 대책	보안감사	

3. VoIP-ITSP(인터넷전화사업자) 연동시 보안

경찰청 VoIP망 ITSP망간의 연동은 고려해야 할 요소들이 몇 가지 있다. 특히, ITSP 망과의 연동에 있어서 백본망으로 직접 연동할 것인지 IP-PBX나 액세스 게이트웨이를 통해 연동할 것인지 여부에 따라 보안적 위험이 달라진다. 백본망과 직접연동을 하게 되면 위에서 살펴본 VoIP관련된 모든 보안이 이루어져야 한다. 하지만 IPT장비로 직접 연동될 경우 장비보안만 이루어지면 되므로 여러 위험요소로부터 벗어날 수 있다. 하지만 IPT장비와의 직접연동 방식은 ITSP 호에 대한 제한이 따를 수 있다. 왜냐하면 모든 호가 액세스 게이트웨이나 IP-PBX에 집중되므로, PSTN, 내부 호처리등 추가적인 부하가 발생될 수 있기 때문이다.

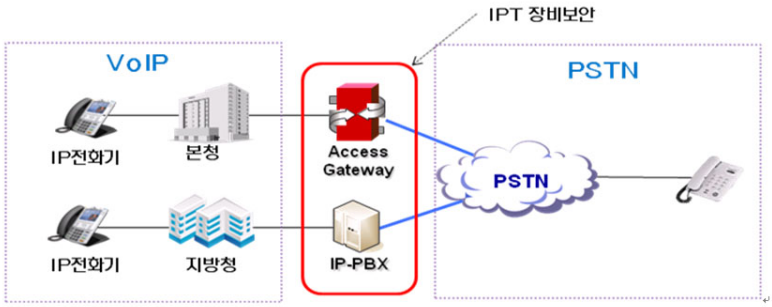
이러한 이유로 IPT장비와 직접 연동시에는 처리용량에 대한 충분한 고려가 있어야 한다.

4. VoIP-PSTN(사업자) 연동시 보안

VoIP망과 PSTN(사업자)망간의 연동에서 있어서 보안은 최대한 연동 포인트를 줄이는 것이 관건이다. 그리고 IP-PBX 또는 게이트웨이 장비가 직접적으로 PSTN과 연동되므로 장비에 대한 보안 대책이 필요하다. 장비에 대한 보안은 기본적으로 IPT 보안을 따른다.

경찰 전화망 구축 시 VoIP-PSTN 연동 포인트를 어디에 두느냐에 따라서 보안적인 위험요소가 달라진다. 아래의 그림과 같이 본청 및 지방청의 경우는 액세스 게이트웨이 또는 IP-PBX에 직접적으로 PSTN 망과 연동이 되므로 장비의 보안 및 시그널링 암호화, 음성 통화에 대한 암호화가 이루어져야 한다.

〈그림 66〉 VoIP-PSTN(사업자) 연동시 보안



지방청 이하의 경찰서나 직할대의 경우 PSTN망과 직접적인 연계를 가지지 않고, 백업 용도로 PSTN과 직접 연결한다. 본청 및 지방청 IP-PBX 가입자인 VoIP 단말 사용자가 보안 대상이 된다.

IPv6 도입 시 중요하게 고려되어야 할 사항 중의 하나는 기존 IPv4 망과의 연동문제이다. 이러한 문제 해결을 위해 IETF에서는 NGTrans, V6ops 워킹그룹을 별도로 두어 IPv6와 IPv4 연동을 위한 다양한 전환 매커니즘(Transition mechanism)을 개발 중에 있다.

또한, 현재 개발된 IPv4/IPv6 전환 매커니즘에서의 중요한 고려 사항 중 하나는 보안 문제에 있다. IP 프로토콜이 처음 개발되어 제안된 1970년 이후, IP 보안에 대한 문제는 끊임없이 지속적으로 연구되어 왔으며, 현재도 인터넷의 가장 취약한 문제점 중의 하나로 보안 문제를 꼽고 있을 정도로 많은 연구와 관심이 진행되고 있는 분야 중의 하나이다.

그러나, 최근 IETF 내의 보안 그룹 등에서 IPv6 프로토콜에서의 확장 헤더의 사용, IPv4/IPv6 전환 매커니즘의 사용시 보안 문제가 발생할 수 있다고 연구결과를 발표하고, 이에 대한 보안 확인을 반드시 하도록 권고하고 있다.

IPv6 도입에 따른 보안 위협 요소를 크게 두 가지로 구분할 수 있다.

첫째, IPv6 프로토콜 자체에 대한 문제로 처음 설계 당시 기존 IPv4와는 다른 확장된 프로토콜을 설계하고자 추가했던 기능들이, 보안 관점에서 문제가 되는 것으로 보고되고 있다.

물론 이러한 문제점들은 IPv6의 궁극적인 문제들이 아니며, 기존 IPv4 프로토콜 역시 해커들의 공격과 이에 대한 보안 문제의 해결이라는 반복을 통해 보다 안전한 프로토콜로 발전해 나갔던 것처럼 IPv6 역시, 이러한 보안 문제점들도 IPv6 프로토콜의 보안기능 수정과 방화벽, 침입방지시스템(IPS)에서의 관련 기능 추가 등으로 인해 해결될 수 있다.

둘째, IPv4/IPv6 연동 환경에 따른 보안 문제들로서, 실제 IPv4 프로토콜, 혹은 IPv6 프로토콜 자체로는 문제가 없지만, 두 망이 혼재되는 상황에선 예상치 못했던 보안 위협 문제가 발생될 수 있다.

〈표 30〉 적용환경별 IPv4/IPv6 전환 메커니즘

적 용 환 경		전환 메커니즘	표준문서
IPv4 망을 경유한 IPv6 단말간의 통신 (IPv6-over-IPv4)	사이트 내(intra-site)	설정터널	RFC 4213
		6to4	RFC 3056
	사이트 간(inter-site)	ISATAP	RFC 4124
	NAT traversal 지원	Teredo	RFC 4380
IPv4 망을 경유한 IPv6 단말간 통신 (IPv4-over-IPv6)		DSTM	1-D(초안)
IPv4 단말과 IPv6 단말간의 통신 환경 (IPv6-to-IPv4 또는 IPv4-to-IPv6)		NAT-PT	RFC 2766
		DSTM	1-D(초안)

출처 : 전자통신동향 분석, ETRI, 2006

1. IPv6 프로토콜 보안 위협 요소

IPv6는 자체적으로 보안 프로토콜인 IPSec을 내장하도록 하여 보안 문제를 근본적으로 해결하려는 시도를 하고 있으므로 IPv4에 비해 보안 상 장점이 있는 것으로 볼 수 있다. 그러나 그럼에도 불고하고 IPv6의 특징으로 기인한 보안상 문제점도 몇 가지가 논의되고 있으며 IPv4-IPv6 전환 과정에서 발생 할 수 있는 보안상 허점 가능성에 대한 것은 또 별개의 영역으로 논의가 진행 중이다.

IPv6 프로토콜 자체에 대한 보안 위협 요소들을 아래 〈표 31〉과 같이 정리된다.

〈표 31〉 IPv6 프로토콜 보안 위협 요소

IPv6 프로토콜 보안 위협 요소	보안 관련 문제점
확장헤더	라우팅 헤더, 홉-바이-홉, 목적지 옵션, 프래그먼트 확장 헤더를 이용한 DoS 공격
다양한 주소 처리	방화벽/IPS에서의 링크-로컬(link-local), 유니크 로컬(unique-local), 글로벌(global) 등 주소별 의미적 필터링 미정의
ICMPv6/ND	RA/RS, NA/NS 메시지들의 안전한 전송 필요, 주소 보안 확장 방법을 이용한 DDoS 공격
멀티캐스트/ 애니캐스트	멀티캐스트 패킷 오류에 대한 응답 메시지 범람 및 애애니캐스트 의미적 필터링 미정의
IPSec 사용	글로벌 점대점 IPSec 사용을 위한 PKI, 키교환 방법 미정의
MIPv6	방화벽/IPS에서의 BU, RR 패킷 차단

2. IPv6 프로토콜 자체의 보안 위협 요소

IPv6의 확장된 주소 범위로 인하여 취약한 호스트를 찾기 위한 포트 스캐닝이 어렵다는 장점이 있는 반면에 역으로 공격자를 추적하는 것 또한 그만큼 어렵다는 단점이 존재한다. 침입 차단 시스템과 침입 탐지 시스템은 IPv6의 새로운 기능 및 보안 기능 처리를 위한 CPU 오버헤드로 인해 서비스 거부 공격의 대상이 될 가능성이 높다는 점도 유의해야 할 대목이다. 또한 라우팅 헤더 등의 확장 헤더를 악용하여 침입 차단 시스템을 우회할 가능성도 있다. 그리고 공격자는 IPv6주소 자동 설정 기능을 악용하여 정상적인 주소 할당을 방해 하거나 정상적인 세션을 종료시킬 가능성도 존재한다.

3. IPv4-IPv6 전환 과정에서의 보안 위협 요소

첫째로 Dual Stack화 된 네트워크 내에서 볼 때 IPv4에서 요구되던 보안 수준이 IPv6에서도 동일하게 적용될 수 있는지 여부가 문제가 될 수 있다. 이러한 보안적인 고려사항 때문에 Dual Stack이라는 단순한 구성을 적용하는 데에도 미처 생각지 못한 시간과 비용이 추가로 발생할 가능성도 있다. 그리고 Tunnel 기법을 활용할 때도 Tunnel은 침입차단/탐지 시스템을 우회하는 도구로서 활용될 가능성이 있다는 점 또한 유의해야 한다. 그리고 마지막으로 Translating 기법 사용 시 IPv4/IPv6 프로토콜 변환은 네트워크/전송/응용 모든 계층에서 발생하며 계위에 따라 다양한 보안 위협 요소가 존재하는 것으로 알려져 있다. 그리고 Translating 작동 과정 중에는 IP헤더의 체크섬 사용이 불가 하거나 prefix 할당 시 보안 취약성, 소스주소 스푸핑 가능성 등의 위협 요소가 존재한다.

4. 보안 위협에 대한 대응

이러한 다양한 보안 위협에 대해서 여러 가지 IPv6 용 정보 보호 기술이 연구 개발 되고 있다. 즉 IPv4/IPv6 변환 용 네트워크 노드 자체에 대한 보안 기술, IPv6 프로토콜 자체에 대한 옵션처리 미적용으로 인한 공격을 방지 할 수 있는 보안 게이트웨이 기술, 그리고 IPv6 프로토콜을 적용한 전용 보안 기술이 연구되고 있다. 한편 정보통신부에서는 다음과 같은 IPv6 보안 기술 개발 로드맵을 발표한 바 있다.

〈표 32〉 정보통신부의 IPv6 보안 기술 개발 로드맵

시 기	내 용
1단계('05)	인트라넷용 유무선 IPv6 정보보호 기술 개발 DNSSEC 기술 개발 IPv6(IPsec) 표준적합성 시험기술 개발
2단계('06~'07)	인터넷용 통합 유무선 IPv6 정보보호 기술 개발 DNSSEC 기술 개발 IPv6(IPsec) 표준적합성 시험기술 환경 구축
3단계('08)	유비쿼터스용 유무선 IPv6 정보보호 기술 개발 DNSSEC 기술 개발 IPv6(IPsec) 표준적합성 시험 시범 서비스

제7장 기타 고려사항

제1절 단말

최근 몇 년 전부터는 기업용 전화로 IP텔레포니 기술을 기반으로 인터넷전화가 꾸준히 증가하고 있다. PSTN 전화를 유·무선 IP전화기로 대체되고 있고, VoIP(WiFi)와 이동전화가 결합된 형태의 단말이 보급되고 있다. 해외에서는 이미 휴대폰에 무선랜(WiFi) 칩을 탑재해 이를 사무실 전화로도 이용하는 것이 대세로 자리를 잡고 있다. 회사 안에서는 이 듀얼모드 휴대폰으로 무료인 VoIP 서비스를 사용하고, 사무실 밖에서는 이동전화로 업무용 통화를 하는 것이다.

하지만, 이러한 이기종 무선환경에서의 서비스 지원은 다음과 같은 문제점을 가지고 있다. 무선의 특징상 보안에 매우 취약한 점, 그리고 단말이 고정되어 있지 않기 때문에 이동성 문제가 따른다. 그리고 다양한 부가서비스 및 이동성을 지원하기 위해서는 IPv6를 지원해야 한다. 이러한 무선단말의 이동성, 보안, IPv6 지원 문제 및 이기종 무선환경에서의 서비스 지원 문제는 경찰에서도 통합단말을 적용하기 위해서는 반드시 해결되어야 할 것이다.

1. 무선 단말의 보안

경찰업무상 음성통신 보안은 반드시 보장되어야 한다. 무선 환경은 유선에 비해 보안상 취약점이 훨씬 심각하다. 특히 이동 환경에서의 보안은 매우 중요하다. 이러한 무선 단말의 보안의 취약성을 해결하기 위해 IEEE 802.11i TG(Technical Group)를 중심으로 사용자가 AP(Access Point)를 핸드오프하는 환경에서도 견고한 실시간 보안 서비스를 제공할 수 있도록 표준 규격을 개발하고 있다.

IEEE 802.11i 표준은 무선 단말의 고정 통신에 대해서는 효과적인 보안 기능을 제공하지만, 향후에 보다 완전한 무선랜 시스템의 보안을 위해서는 무선 단말의 신속하고 안

전한 이동성을 보장하는 이동 보안 측면에서는 더욱 발전된 기술이 필요하다. 선인증(Pre-authentication)과 마스터 키(PMK) 관련 정보의 캐시(cache)가 이동 보안을 위한 기초적인 기능을 제공하고 있지만, 이는 실시간 핸드오프를 요구하는 VoIP(Voice over IP) 등의 응용에서는 보완이 필요할 것으로 보인다.

2. 무선 단말의 이동성(Mobility)

이기종 무선환경 및 무선 AP 커버리지를 벗어날 수도 있으므로 이동 시에도 통화가 끊기지 않도록 단말의 이동성에 대한 고려가 필요하다. 노트북과 같은 비교적 크고 무거운 단말은 이동성과는 거리가 멀지만 PDA, Wi-Fi Phone 과 같은 형태의 단말을 고려한다면 이동성은 중요한 기술적 고려사항이 된다. 무선랜의 이동성은 AP간의 로밍 문제와 직결된다.

〈그림 67〉 Seamless IP Mobility

위의 그림은 무선단말이 WiFi망에서 WiBro망으로 이동할 때의 끊김 없는 통화를 위한 IP 이동성을 보여주는 것으로 WiFi와 WiBro가 공존하는 구간에서 WiBro 신호가 더 강해지는 쪽으로 이동될 때 기존의 연결을 해제하고 WiBro로 AP를 통하여 통신하는 것을 보여준다.

이처럼 끊김 없이 통화가 이루어지지 WiFi구간에서 WiBro구간으로 넘어 갈 때 재인

증이 이루어지면 안 된다. 왜냐하면 인증과정에서 새로운 IP주소를 부여 받기 때문에 기존 세션이 종료되어 통화가 단절되기 때문이다.

3. IPv6 지원

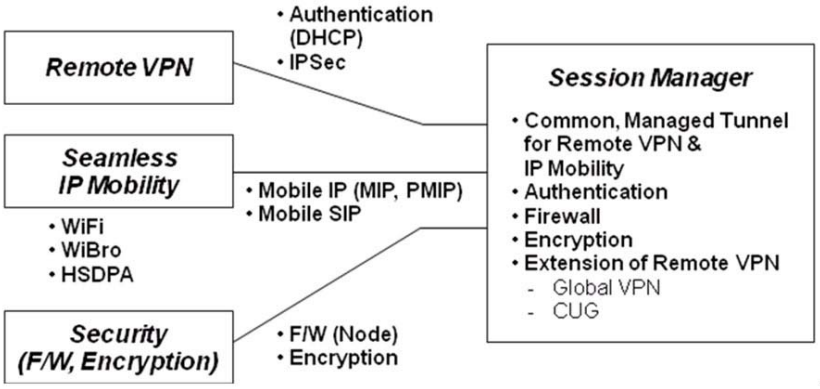
인터넷의 성장과 무선기술의 발전으로 인해 무선 인터넷에 대한 사용자의 요구는 급증하고 있다. 무선 인터넷 서비스를 제공하기 위한 기반 네트워크는 회선 방식, 음성 위주의 서비스에서 패킷 방식, 데이터 서비스 위주의 IP 기반 네트워크로 발전하고 있다. IPv6가 무선 인터넷 분야에서 필요성이 대두되는 이유는 다양한 이동 단말의 IP 주소 요구량을 현재의 IPv4 주소체계로는 감당할 수 없기 때문이다. 또한 IPv6는 IPv4에 비해 효과적으로 이동성을 지원할 수 있는 특징들을 가지고 있어서 IPv6 도입은 필수적이라 할 수 있다.

3GPP2에서는 이동전화 네트워크와 패킷 네트워크가 별도로 존재하는 현재의 구조에서 이 두 네트워크가 하나의 IP 네트워크로 통합되는 All-IP 개념을 제시하고, 세부적인 표준화 작업을 진행 중에 있으며, All-IP 네트워크에서 단말의 효과적인 이동성 지원을 위해 Mobile IPv6를 표준으로 채택한 상태이다.

4. Session Manager

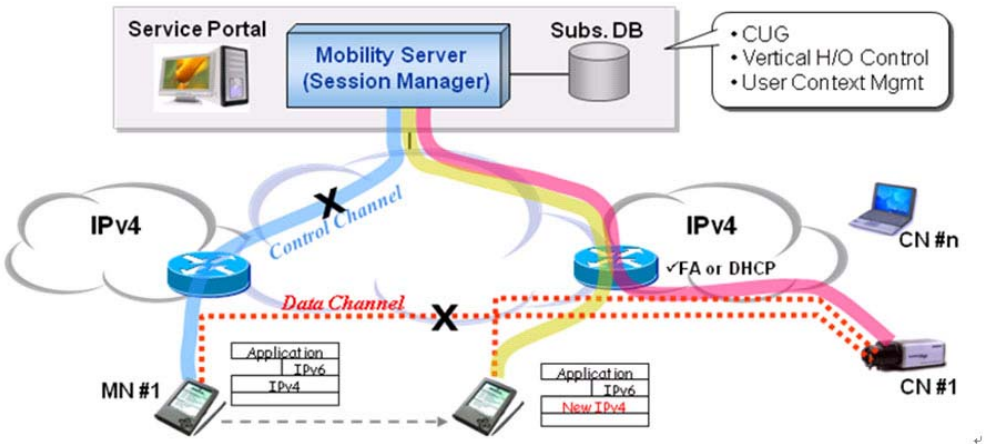
이처럼 무선단말의 보안, 이동성, IPv6지원할 수 있는 대안 기술로써 Session Manager 기술을 소개한다. Session Manager는 Remote VPN과 IP 이동성을 위한 터널관리 그리고 인증과 파이어월, 암호화, 확장 Remote VPN(CUG, Global VPN)등을 지원할 수 있는 기술이다. 특히 이기종 무선기술간의 IP 이동성을 제공하기에 적합한 기술로서 아래의 그림과 같이 인증 및 IPSec, 이기종 무선망(WiFi, WiBro, HSDPA) 간 Seamless IP Mobility를 지원할 뿐만 아니라 보안 터널을 통한 이동단말의 보안 문제 또한 해결 가능하다.

〈그림 68〉 Session Manager



〈그림 67〉은 단말의 IP 이동성을 보여주는 것으로 IPv4망에서 IPv6서비스를 제공하는 것을 보여준다. 특히, Session Manager는 각 단말의 정보를 DB에 저장하고 있다가, 단말이 이동했을 때 Secure 터널을 통해 재인증을 하지 않고, 끊김 없이 통화가 유지되도록 한다.

〈그림 69〉 Session Manager(Secure P2P Signaling)



제2절 품질(QoS)

1. VoIP 통화 품질

기존 PSTN 통화품질은 회선을 점유하는 방식이므로 대역폭 문제는 존재하지 않았다. 네트웍 자원을 공유하지 않기 때문이다. 하지만 IP기반 망은 회선을 공유하는 특징 때문에 통화품질에 관련된 문제가 발생된다. 특히, 실시간 통신서비스인 음성 및 영상 서비스는 충분한 대역폭을 가지지 못한다면 품질저하의 요인 될 수 있다.

이처럼 PSTN 회선을 IP망으로의 전환시에 안정적인 품질 보장, 그리고 IP 네트워크를 위한 신규 서비스 속성별 품질보장이 가능한 QoS 네트워크로의 전환이 필요하다. 현재의 IP망 구조에서는 기존 PSTN 통화품질 수준을 그대로 제공하기는 사실상 어렵다. 그래서 신규서비스에서 요구하는 서비스 품질 수준을 최대한 만족하기 위해서는 다양한 서비스 별 차별화가 가능한 QoS 적용환경 구축이 필요하다.

다음 표는 VoIP 환경에서의 통화품질을 코덱별로 비교한 것이다.

〈표 33〉 Codec에 따른 통화품질(MOS)

코덱종류	Bit Rate (BW)	인코딩 타임	MOS	비 고
G.711	64 kbps	10 ms	4.1	PSTN 통화 품질
G.729	8 kbps	10 ms	3.92	VoIP에서 주로 쓰임
G.723.1	6.3 kbps	30 ms	3.9	압축률이 높음
G.723.1	5.3 kbps	30 ms	3.8	압축률이 높음
G.726	32 kbps	5 ms	3.85	BW 높을수록 좋음
G.728	16 kbps	5 ms	3.61	

PSTN은 ITU-T G.711 코덱을 사용하기 때문에 대역폭이 64Kbps인데 반하여, VoIP에서 주로 쓰이는 코덱인 G.729의 경우 8kbps이기 때문에 전송자원 측면에서 효율이 높다. 하지만 위에서도 언급했듯이 회선을 공유하는 방식 때문에 트래픽이 폭주했을 때 안정적인 대역폭 확보가 이루 지지 않는다면 통화품질을 보장할 수 없는 문제를 가지고 있다. 이처럼 통화품질을 보장하기 위해서는 트래픽별 QoS 제공이 가능한 기술이 필요하다.

2. 네트웍 서비스 품질보장 기술

IP 네트워크 아키텍처에서 서비스 품질 보장을 위한 많은 시도가 이루어지고 있으며, 대표적으로 Diffserv, Diffserv over MPLS, DS-aware TE 의 순으로 발전되어 왔다.

- DiffServ: Diffserv 개념은 네트워크의 입력량과 출력량에 대한 적절한 조절이 가능하면 네트워크의 상태에 따라 동적으로 경로가 결정되는 IP 네트워크에서 일정수준의 서비스 품질을 보장할 수 있다는 관점에서 제기된 개념이다. 그러나 이 개념은 모든 링크에 대한 자원 사용 현황이 실시간적으로 반영이 되지 않으면 필연적으로 발생하는 체증현상에 대한 제어성에 문제를 내재하고 있다.
- DiffServ over MPLS (E-LSP): DiffServ 의 결함을 보완하기 위하여 Edge부터 Edge까지 파이프(MPLS E-LSP)를 구성하여, 파이프 내에서의 차별적 서비스를 제공하자는 Diffserv over MPLS 개념으로 발전되었으나, 상용 라우터들의 큐잉 및 스케쥴링 방식의 문제로 인하여 transit node 에서 필연적인 체증 현상이 발생하는 문제를 가지고 있다. 일반적으로 파이프는 파이프내의 트래픽을 보호하기 위하여 파이프 단위의 weighted fair queuing을 제공하여야 하나, 상용 라우터들이 class-based queuing과 스케쥴링을 제공하기 때문에 파이프를 설정해도 파이프내의 트래픽을 보호할 수 없어 MPLS 를 도입하고도 over provisioning 에 의존할 수 밖에 없다. 상식적으로 파이프라는 개념은 파이프내의 트래픽을 보호하고 파이프에 트래픽을 인가시키는 단계에서 등급단위로 차별적으로 인가시키면 자연스럽게 파이프 내에서의 차별적 서비스는 자동적으로 제공할 수 있으나, 패킷까지 우선순위를 적용하는 변형된 구조를 가지게 된 것은 IETF 의 E-LSP 에 대한 RFC가 상용 라우터의 한계를 교묘하게 숨기는 차원에서 만들어졌다는 것을 확인시켜주는 것이다.
- Flow 기반의 QoS 보장 네트워크는 분산제어 방식의 제어성과 신뢰성 문제를 극복하기 위하여 토폴로지 및 네트워크 자원에 대한 관리는 집중형을 기본으로 한다. 사용자가 네트워크의 자원 예약을 필요로 하는 고품위 서비스를 이용하기 위해서는 반드시 호 수준 또는 Path 수준의 수락제어(Call/Path Admission control) 과정을 거쳐야 한다. 네트워크의 안전성 확보를 위하여 사용자가 전달 장비에 대한 직

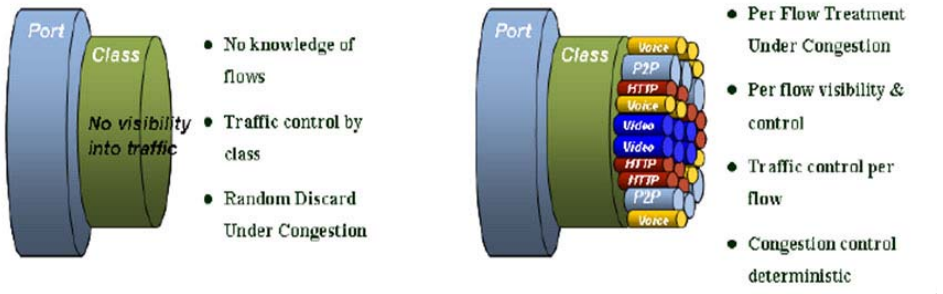
접적인 자원 협상을 하는 것은 배제한다. 또한, 모든 패킷은 subdomain 단위 또는 네트워크 계위 단위의 경계점을 제외하고는 집중형 자원관리체계에 의하여 사전에 설정된 VSP(Virtual Switched Path: LSP 의 일반화된 개념)에 인캡슐되어 전달된다. 아울러 VSP 로 구성되는 논리 네트워크는 전달장비로부터 모니터링된 자원 사용 정보를 바탕으로 자동적으로 최적화된다.

3. 경찰 네트워크 QoS

경찰 네트워크에 품질을 보장하기 위해서는 다양한 서비스별 우선 순위에 따라서 트래픽을 제어할 수 있는 기술이 필요하다. DiffServ 는 근본적으로 보장 서비스(Guaranteed Service)에 대하여 한계점을 가진다.

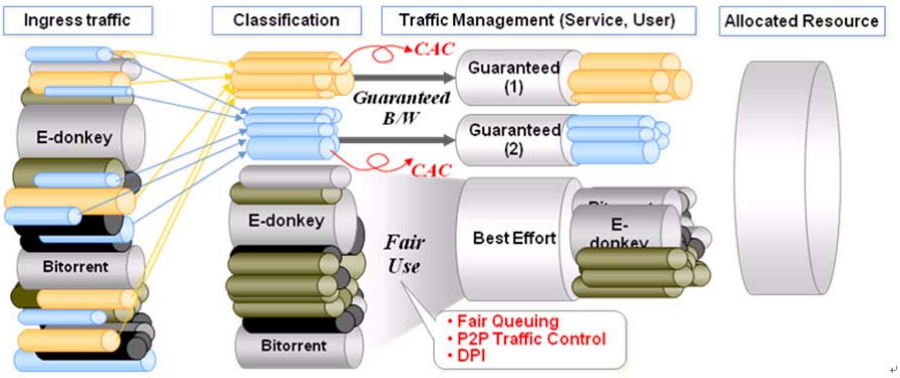
경찰 네트워크에는 플로우별 QoS를 보장할 수 있는 플로우기반 QoS 기술이 적합하다. 이러한 플로우별 QoS 처리 방식은 아래의 그림에서 보여주듯이, 다중 큐에서 유입되는 플로우에 대해서 스케줄러가 설정된 플로우 프로파일 정보를 바탕으로 각 클래스 단위로 트래픽을 처리하여 QoS를 제공하는 방식보다 우수한 성능을 나타낸다.

〈그림 70〉 클래스별 QoS방식 vs. 플로우별 QoS 방식



플로우 기반 QoS 기술은 특히, 신규 서비스의 요구 품질기준을 최대한 만족 시키고, 다양한 서비스별 차별화가 가능한 QoS 적용 환경 구축에 적합할 것이다. 또한 망 고도화 추이와 서비스 확산 추세를 반영한 점진적인 확대 적용이 가능하다. 또한, 다양한 트래픽이 혼재되어 있는 광대역 통합망에서 서비스에 대한 품질을 보장하는 기술로 적합할 것이다.

〈그림 71〉 End-to-End QoS



위의 그림과 같이 트래픽이 혼재되어 있는 경우, 품질보장을 요구하는 서비스에 대해서는 서비스 트패픽를 분리하여 충분한 대역폭을 제공해 서비스 안정성을 보장해주는 Guaranteed 서비스가 제공되고, P2P와 같은 품질보장이 요구되지 않는 서비스에 대해서는 대역폭을 공유하는 Best Effort 서비스가 이루어 진다.

제8장 결 론

정부의 u-IT839 정책에 따라 기존의 전화망(PSTN)이 차세대 통신망(IP 네트워크)으로 전환됨에 따라 기존의 일반 전화가 IP전화로 자리 바꿈하고 있고, 이 속도는 점점 가소화 되고 있다. 이러한 PSTN 기반의 통신망이 고품질 영상전화, 멀티미디어 서비스, 통신비용 절감 등의 목적으로 기존의 음성, 데이터, 영상, 무선 등의 서비스가 통합되고 있다. 이러한 서비스의 변화에 따라 경찰전화망도 업무 효율성 증대와 대국민 치안 서비스 등의 필요성에 따라 활용도 높은 IPT 시스템 기술이 도입되어야 한다. 그리고 기존 전화망의 문제점인 전화번호 자릿수 문제와 IPT도입에 따른 체계적인 번호설계가 필요하다. 또한, 폭발적인 단말의 증가가 예상됨에 따라 기존의 IPv4 주소체계 한계가 있으므로, 신 인터넷 주소체계인 IPv6의 도입이 시급하다. 하지만, 경찰통신망 고도화에 따른 몇 가지 고려해야 할 사항들이 있다. 특히, PSTN 기반망에서 All-IP 망으로 진화함에 따라 경찰통신망에 한층 업그레이된 보안이 필요하며, IPT 도입에 따른 문제점인 이기종 장비간의 연동 문제 및 다양한 망간의 연계 문제가 해결되어야 할 것이다.

이에 본 보고서에서는 경찰전화망 전화번호 체계의 문제점과 고도화에 따른 문제점을 분석하고, 새로운 전화번호 체계 및 내선번호 체계를 제시하였다. 또한 IPv4에서 IPv6로의 전환에 위한 Subnet 부여방안과 IPv6로 이행방안, 그리고 경찰통신망의 보안서비스 설계 방안을 제시하였다.

이러한, 신기술 및 새로운 기능 그리고 이기종 장비간의 적합성을 검증하기 위한 시범사업 과 테스트베드 구축, 그리고 각각의 솔루션 비교 및 분석하여 가장 적합한 기술을 도입할 수 있도록 기반이 마련 되어야 한다. 그리고 단계적으로 신기술이 도입되는 과정에서 발생되는 기존 시스템과의 공존에 대한 대책이 마련되어야 한다.

향후 앞에서 제시한 내용을 기반으로 한 테스트베드 구축과, 상세설계가 이루어져야 할 것이며, 경찰 통신망에 적합한 IPv6 기반 서비스 발굴과, 무선환경에서의 보안 문제 해

결을 위한 R&D 사업이 추진되어야 한다. 또한 USN연동, 디지털 TRS, 무선망연동, QoS(품질관리)등에 대한 많은 연구가 필요할 것이다.

1. IPv6 표준화 현황 및 개발 동향

IPv6는 1996년 IETF(Internet Engineering Task Force)에 의해 표준화 되었다. IETF는 90년대 초반에 품질관리의 문제를 해결하기 위하여 IPv5 규격을 검토한 이후에 보안기능과 자동 네트워킹 기능 등을 보완하여 1996년에 IPv6(RFC2460)을 표준으로 규정하였다. 이후 많은 워킹 그룹을 통하여 표준화 작업을 진행 중이며, 2005년 8월 프랑스 파리에서 개최 되었던 IETF 63차 회의에는 36개국의 1454명이 참가하여 4개의 새로운 워킹그룹을 구성 하였고 548개의 새로운 초안기고를 제출하였으며, 103개를 최종검토로 요청하는 등 활발한 표준화 활동을 하고 있다. IPv6 표준화는 IPng과 NGTrans WG을 중심으로 진행되고 있다. 우선 IPng WG은 IPv6 기본 프로토콜 구조에 관한 규격을 제정해온 그룹으로 IPv6 기본규격과 IPv6 주소 자동 생성에 관한 표준을 제시하였다. NGTrans WG은 IPv4망에서 IPv6 적용 및 IPv6로의 전환을 위해 기존 망과의 상호 운용에 필요한 전환 메커니즘에 대한 표준화를 담당해 왔으며, 현재는 v6ops WG으로 명칭을 변경하여 IPv6로의 전환 시나리오 작업과 IPv6 운용과 IPv6 응용 개발에 대한 가이드라인을 표준화하고 있다. 이 밖에 IPv6 관련 IETF WG으로는 IP 계층의 트래픽 보안에 대한 구조 정의나 보안 관련 관리와 인터넷상에서 암호화 키 설정에 관련된 표준 등을 연구하고 있는 IPSec WG과 IP 이동성 지원에 대한 표준화 활동을 전담하고 있는 Mobile IP WG 등이 있다. 현재 활동 중인 주요 IETF 워킹그룹과 활동 내용은 다음 〈표 34〉과 같다.

〈표 34〉 IPv6 관련 IETF 워킹그룹 현황

WG	활 동 내 용
IPv6	IPng WG의 역할을 승계하여 IPv6프로토콜에 대한 표준화 담당
v6ops	NGTrans WG의 역할을 승계하여 IPv6네트워크를 도입하기 위한 기술 및 시나리오 가이드라인 제시
MIP6	Mobile IP WG의 역할을 승계하여 IPv6노드가 이동 중 Home address를 지속적으로 사용하는 것을 허락하도록 하는 라우팅 지원
DHCP	IP주소와 TCP/IP Stack의 매개변수 자동할당, 설정 및 관리하는 DHCP 개발
MANET	Mobile Ad-Hoc 환경에서 이동단말들 간의 통신에 필요한 라우팅 프로토콜 개발
MAGMA	Multicast, Anycast와 같은 Group Management 프로토콜 개발
DNSext	DNS관련 기술 표준 연구
VRRP	IPv4/IPv6에 대한 VRP 연구
MEMO	기기 단위로 움직이는 전체 네트워크에서 인터넷 접속방법 연구
NSIS	IP 신호 프로토콜 표준화 담당
SEND	IPv6 Neighbor Discovery 의 보안을 위한 프로토콜 연구
DNSop	DNS name server 와 DNS zone file 작동에 관한 가이드라인 제시
MIPSHOP	Mobile IPv6의 시그널링 오버헤드와 핸드오프 지연/패킷손실 이슈 관련 HMIPv6와 FMIPv6등의 기술
DNA	IPv6자동설정에서 라우터 탐색 및 망관련 지연 감소 또는 방지를 위한 메커니즘 개발
multi6	IPv6에서 장애관리 및 부하분산을 위한 Multi-homing 방법 관련 문제 담당

국내에서는 IPv6포럼 코리아, 개방형컴퓨터통신연구회(OSIA) 등의 지원을 받아 TTA가 IPv6 기본규격들에 대한 국내 표준안의 개발 업무를 수행중이다. 2003년 초에 처음으로 IPv6 기술표준 개발을 전담하는 IPv6 전담반이 구성되어 총 8건의 국내 단체표준을 제정하였고 현재 총 40건의 IPv6관련 국내 단체 표준이 제정 중이다. 국내에서 추진중인 IPv6 표준화 과제 현황은 〈표 35〉와 같다.

〈표 35〉 IPv6관련 국내 표준화 추진 과제 현황

표준화 과제명	제 안 처	국제표준
IPv6 주소체계 표준(안)	ETRI	RFC3513
RADIUS와 IPv6	SG02.02	RFC3162
PPP상에서의 IPv6패킷전송	ETRI	RFC2472
역탐색을 위한 IPv6 인접탐색 확장	IPv6포럼코리아, ETRI	RFC3122
IEEE1394 네트워크 상에서의 IPv6패킷 전송	IPv6포럼코리아, ETRI	RFC3146
BIS기법을 사용한 듀얼스택 호스트 기법	IPv6포럼코리아, ETRI	RFC2767
IPv4망을 경유한 IPv6도메인간의 연결기법(6to4)	TF02.09	RFC3056
IPv6 호스트와 라우터를 위한 전환 메커니즘	TF02.09	RFC2893
네트워크 주소 및 프로토콜 변환기법(NAT-PT)	IPv6포럼코리아, ETRI	RFC2766
상태 비보전형 IP/ICM 변환 알고리즘	IPv6포럼코리아, ETRI	RFC3765
3GPP에서의 IPv6권고사항	ETRI	RFC3314
IPv6주소 집합과 재할당 지원용 DNS확장	IPv6포럼코리아, ETRI	RFC2874
IPv6를 위한 기본 소켓 인터페이스	TF02.09	RFC3493
IPv6를 위한 확장 소켓 인터페이스	TF02.09	RFC3542
IPv6 디폴트 주소 선택 기법	ETRI	RFC3484
IPv6를 위한 라우팅 주소 재할당	IPv6포럼코리아, ETRI	RFC2894
IPv6 over CDMA에서의CDMA/WLAN이종간 인터워킹	PG210	RFC3122
IPv6 over CDMA에서의 IPv6 주소할당정책	PG210	RFC2472
IPv6 over CDMA에서의 IPv6/IPv4 네트워크 전화기법	PG210	RFC2373

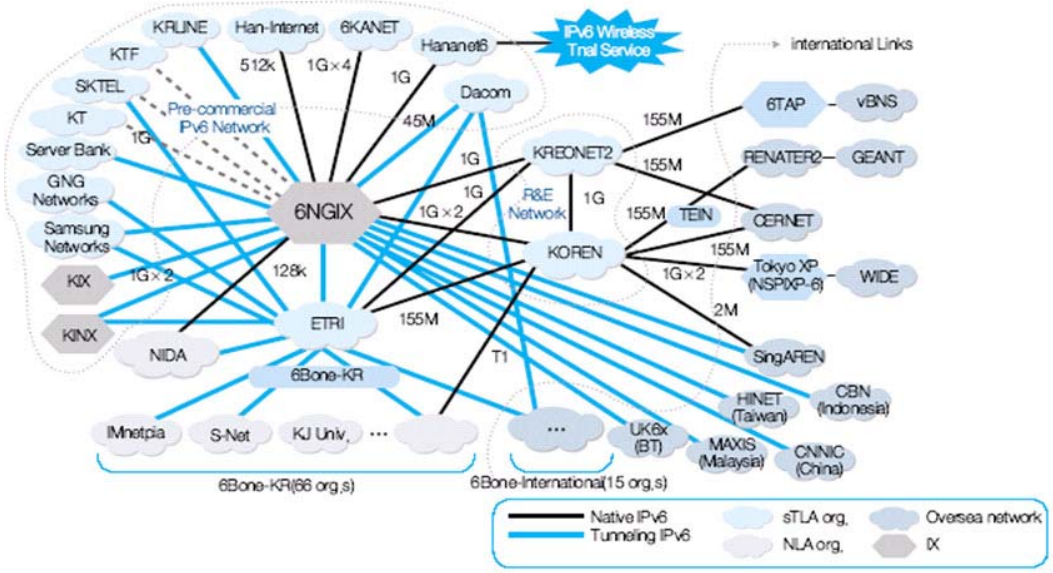
또한 정보통신부가 IPv6의 보급과 지원을 위한 정부 측 대표기관으로 정통부장관을 위원장으로 하는 IPv6 전략 협의회를 구성하고 있고, 한국정보사회진흥원, NIDA, TTA, ETRI 등에서 IPv6와 관련하여 연구 및 개발, 시험/인증, 주소할당, 사업발굴 등의 사업을 진행 중이다.

IPv6 장비 및 솔루션 개발도 국내외적으로 매우 활발히 진행 중이다. 국내 업체로는 삼성전자, LG전자, 모다정보통신, 아이엠넷피아, 아이비트 등에서 적극적으로 개발 작업 중이며, 국외 업체로는 CISCO, HITACHI, Microsoft, Hewlett-Packard, Sun Microsystems, IBM, NEC, Nevell, NOKIA, JUNIPER, NTT, 6WIND, FUJITSU 등 대부분의 IT업체에서 IPv6 장비 및 솔루션 개발에 심혈을 기울이고 있다.

2. 국내외 IPv6 Network 및 서비스 현황

IPv6 네트워크는 크게 상용 ISP망과 연구·시험망으로 구분할 수 있으며 이러한 망들 간의 연결을 제공하는 교환노드가 있다. 국내의 IPv6 네트워크 구성은 다음 〈그림 72〉와 같다.

〈그림 72〉 국내 IPv6 네트워크



출처 : IPv6 포럼코리아

상용 ISP망이란 수익을 창출하기 위한 목적으로 ISP가 IPv6망 관련 서비스를 제공하거나 자체적으로 준비하는 망이고, 연구·시험망은 대학 및 연구소 등의 연구기관들을 연결하여 IPv6망을 통한 과제연구에 활용되는 망 또는 이와 더불어 IPv6의 보급 촉진을 위하여 일반인에게 사용기회를 제공하는 망이다. 교환노드는 서로 다른 IPv6망들을 연결해 주는 네트워크로서 Internet eXchange(IX)라고 한다. 다음 〈표 36〉은 국내·외의 대표적인 IPv6 네트워크들을 분류에 맞게 정리한 것이다.

〈표 36〉 IPv6 네트워크 분류

종 류	국 내 망	국 외 망		
		아 시 아	북 미	유 럽
상용 ISP망	KT SK텔레콤 데이콤 하나로텔레콤	NTT IIJ PoweredCom 등	vBNS+ AT&T Qwest 등	LEAnet Nerim 등
연구시험망	6Bone-KR 6KANet KOREN TEIN KREONET2 6GN	WIDE KDDI JENS CERNETv6 6TNet 등	Abilene Moonv6 Cnet4 등	Euro6IX 6net Renater GEANT 등
교환노드	6NGIX KINX	NSPIXP-6 JPIX 등	6TAP 6IIX NY6IX PAIX 등	Euro6IX AMS-IX INXS UK6X Euro-IX 등

출처 : IPv6 Status Report 2004, NCA

가. 상용 ISP 망 현황

국내의 상용 ISP망으로는 KT, SKTelecom, 데이콤, 하나로텔레콤 등이 있으며 각 망별로 다양한 시범 서비스 및 시범 사업을 수행하고 있다.

○ KT

KT는 1999년 APNIC로부터 국내 최초로 공인 IPv6 주소를 확보하고, IPv4/IPv6를 동시에 지원하는 듀얼스택 연구망인 KOREN을 구축하였다. 2000년에는 KOREN에서 IPv6, 멀티캐스트, QoS 서비스 등을 국내 대학 및 연구기관에 제공하였고 2001년에는 무선랜 시험실환경에서 Mobile IPv6 시험을 완료하였다. 2002년에는 IPv6를 KT 인터넷망에 도입하는데 필요한 IPv6패킷 전달방식별 성능시험을 완료하여 2003년 IPv6망 구축방안

마련을 위하여 테스트베드에서 IPv6상호운용성시험을 하였고, IPv6용 침입차단시스템인 Sixwall을 개발하였다. 2004년 6월부터 현재까지는 KOREAv6 시범사업에 참여중이다.

○ SKTelecom

SKTelecom은 IPv6기반의 이동통신 서비스 개발 및 구현을 위하여 IPv6와 Mobile IPv6의 프로토콜 동작 및 기능 테스트 수행을 목표로 IPv6시험망을 구성하였다. IPv6망은 IPv4, IPv6, IPv4/IPv6 Dual Routing을 모두 지원하며 6Bone, 6NGIX와 연동 되어 있다. SKTelecom의 현재 IPv6망은 WLAN망이며 향후에는 CDMA2000-1X/EV-DO, WCDMA, WiBro 및 유선환경에서 응용서비스 개발과 테스트를 위한 시험망으로 사용할 예정이다.

○ 데이콤

데이콤은 2000년 APNIC로부터 IPv6 공인 주소를 획득하여 IPv6 시험망을 구축하였다. 2001년에는 NAT-PT, Tunnel Broker, IPv6 DNS 서버 등의 IPv6 응용서비스를 사내 IPv6망에 적용하여 응용서비스 개발 및 기술 검증을 수행하고 있다. 2002년에 6NGIX, KIDC와 IPv6시험망 연동을 시작하였고 2004년 IPv6환경에서 VoIP 시험을 수행하며 KOREAv6 시범서비스에 참여하고 있다.

○ 하나로텔레콤

하나로텔레콤은 2001년 KRNIC을 통해 /35 bit의 주소공간을 확보하여 상용망 백본에 IPv6 네트워크를 별도로 구성하였고, 6NGIX와 Native로 연결하였다. 2003년에는 무선랜을 기반으로 하는 IPv6네트워크를 구축하여 시범서비스를 제공하였고, IPv6를 통한 영상 및 기타 서비스를 제공하는 "IPv6하나포스닷컴시연사이트"를 운영하고 있다.

국외에서도 유럽과 북미, 일본을 중심으로 많은 상용 ISP 망들이 존재하고 다양한 시범사업이 진행 중이다.

○ 유럽

유럽의 영국에서는 LEAnet가 BT사의 시험망을 이용하여 주소할당, 연결성, QoS 등에 대한 연구를 진행 중이다. 프랑스에서는 Nerim이 ADSL을 통한 Native IPv6서비스, Tunneling 서비스를 IPv4와 같은 비용으로 제공하고 있고, BGP 기술을 활용하여 IPv4/IPv6 전환시스템을 사용하고 있다.

○ 미국

미국에서는 vBNS+가 가입기관들과 OC12~OC48의 백본대역폭과 OC12(ST)의 연동대역폭으로 Native방식 및 Tunneling 방식으로 연결하여 시범서비스를 실시하고 있다.

○ 일본

일본에서는 NTT IPv6에서 IPv6 Gateway, OCN IPv6 Tunneling 서비스, OCN, ADSL Service를 하고 있으며 2004년 10월 Global IP망에서 IPv6/IPv4 듀얼 서비스를 시작하였다. IIJ IPv6 전용회선을 통하여 사용자에게 64Kbps, 128Kbps, 1.5Mbps의 속도로 IPv6 연결을 제공하고 있으며 IPv6 Native, Tunneling, 듀얼스택, Data Center 서비스를 제공하고 있다. PoweredCom에서는 Tunneling, Hybrid, Native 서비스를 제공하고 있으며 IPv6 호스팅 서비스를 테스트하는 중이다.

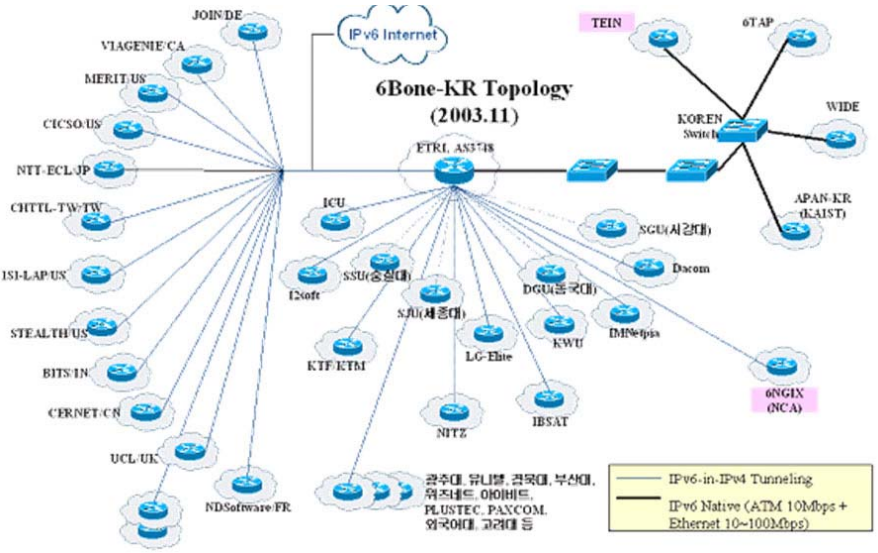
나. 연구 · 시험망 현황

국내 최초의 IPv6 시험망은 1998년 5월 ETRI가 IPv6개발과 연구 촉진을 위해 국제 6Bone으로부터 3FFE:2E00::/24 주소를 할당받아 구축한 6Bone-KR이다.

6Bone-KR은 1999년 7월 APAN-KR로부터 3FFE:8040::/28 주소를 하나 더 할당받아 현재 2개의 IPv6 주소 Block을 보유한 상태이다. 6Bone은 가입 네트워크 확산 및 IPv6 관련 기술과 애플리케이션 개발을 주 활동으로 하고, 국내에서의 6Bone 토폴로지 조정 등 6Bone 네트워크 관리자와 사용자에게 유용한 서비스를 제공하고 있다. 현재 6Bone-KR는 74개 기관과 터널링 또는 Native방식으로 연동되어 있으며 전체 네트워크

구성도는 다음 〈그림 73〉과 같다.

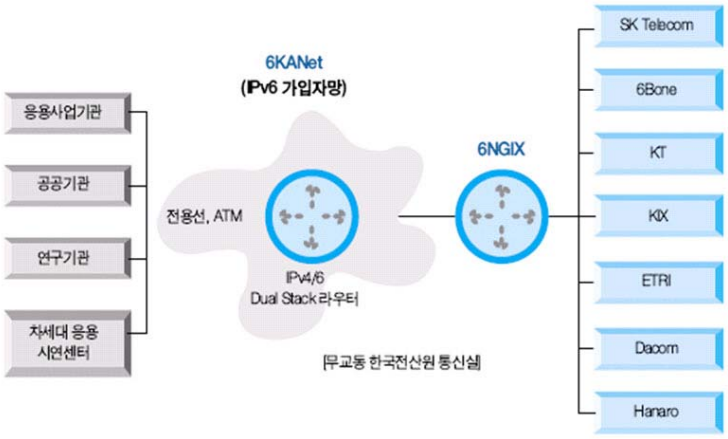
〈그림 73〉 6Bone-KR 네트워크 구성도



출처 : 6Bone-KR,

또 다른 국내의 IPv6 연구시험망으로 6KANet(IPv6 Korea Advanced Network)이 있다. 6KANet은 Native IPv6 및 IPv4를 수용하는 일반 ISP로서의 역할을 수행하며 기본적으로 NLA1(/41) 및 NLA2(/48)의 IPv6주소를 도서관, 관공서, 방송국 등의 기관에 할당하여 IPv6 서비스를 제공한다. 단 IPv6가 확산될 때까지는 보급차원에서 일반 기업을 대상으로도 서비스를 제공할 예정이다. 6KANet은 6NGIX와 연동되어 IPv4는 물론이고 IPv6 인터넷 서비스를 제공하고 있고 현재 6KANet의 가입기관들은 IPv6 messenger 및 간단한 VoD 서비스 등을 홈페이지를 통해 추가로 이용할 수 있다. 2003년 12월에는 백본장비의 성능향상, FTTH APT에 IPv6 서비스 제공, NMS 및 로그서버 구축, Teredo 서버구축 등의 고도화 작업을 실시하였다. 현재 IPv4/IPv6 듀얼스택으로 운영되어 IPv4 서비스도 제공하지만 향후에는 IPv4 서비스는 제공하지 않을 예정이다. 다음 〈그림 74〉은 6KANet의 네트워크 구성도를 나타낸다.

〈그림 74〉 6KANet의 네트워크 구성도



출처 : 6KANet,

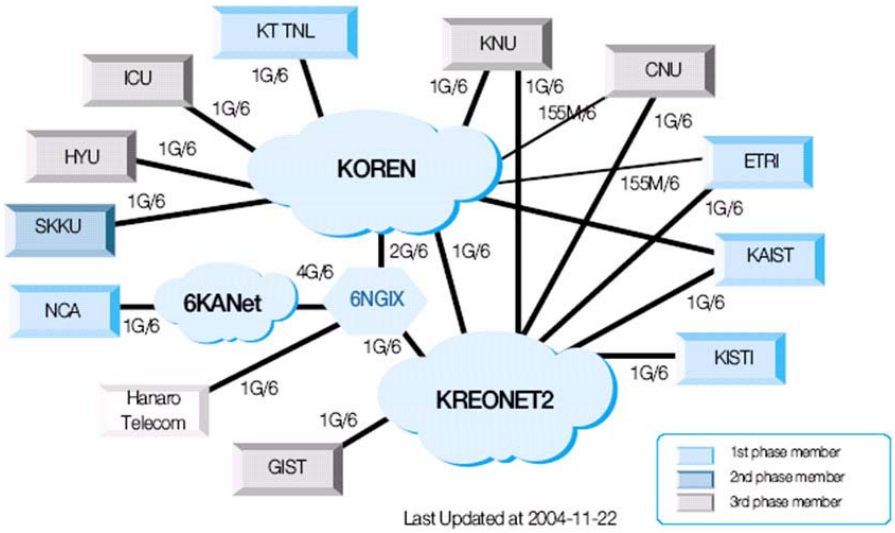
KOREN(KOrea advanced REserch Network) IPv6는 전화선이나 동축 케이블과 같은 기존 네트워크의 한계를 극복하기 위해 초고속 대용량 전송매체인 광케이블과 ATM 교환기를 근간으로 구축된 네트워크이다. KOREN은 Native IPv6 위주의 접속서비스, 국내외의 IPv6 네트워크와의 연동 등을 통하여 상업망으로 가기 이전 단계 수준의 안정적인 IPv6 서비스제공을 목적으로 하며 현재 46개 기관이 이용하고 있다. KOREN은 ATM을 기반으로 광대역의 IPv4 및 Native IPv6 서비스와 멀티캐스트, MPLS, GRID, QoS를 적용한 차세대 인터넷 서비스를 제공하여 왔으며 순차적으로 기가비트 이더넷으로 전환을 진행 중이다.

KREONET2는 KISTI가 1988년부터 국가 연구망인 초고속연구망(Korea Research Environment Open Network: KREONET)의 차세대 연구망으로 국내 및 국제 IPv6 네트워킹서비스를 제공하고 있다. 특히 2004년에는 광 네트워크 통신인 Lambda Based Network에 IPv6를 적용하여 국내에는 대전, 서울, 광주, 대구 등 4개의 네트워크 core 백본을 중심으로 테스트베드를 구축하였으며, 해외망은 중국, 일본, 대만 등 아시아 지역과 시애틀(PNWG: Pacific Northwest GigaPoP)을 통해 북미 지역에 Global Lambda Networking 테스트베드를 구축하여 운영하고 있다.

KOREN과 KREONET2상에서 구현된 논리적인 망인 6GN(IPv6 Gigabit Network)

는 보다 진보된 IPv6 기반 네트워크 인프라에 대한 요구와 Lambda Networking과 같은 진보된 고속 IPv6 망 기술의 신속한 도입 요구에 의해 2003년 12월부터 APAN 및 ANF의 IPv6 Task Force에 의해 추진되어 구축되었다. 진보된 IPv6망의 보급을 위해 우리나라 최초로 기가비트 IPv6 인프라를 구축하였다는 점에서 의미가 큰 6GN은 ETRI, KISTI, NCA, KAIST, KT TNL 등 5개 기관으로 시작하여 2004년 5월까지 Phase1이 진행되었으며, 2004년 12월에는 13개의 가입기관과 2개의 백본, 1개의 교환노드로 확장되었다. 현재 6GN에서는 IPv6망의 성능, IPv6 응용의 개발과 전개, IPv6 망의 모니터링과 관리, IPv6 멀티캐스트 전개, 그리고 KOREAv6 프로젝트 등과 관련된 이슈에 대한 작업이 이루어지고 있다. 6GN의 네트워크 구성은 다음 〈그림 75〉와 같다.

〈그림 75〉 6GN 네트워크 구성도



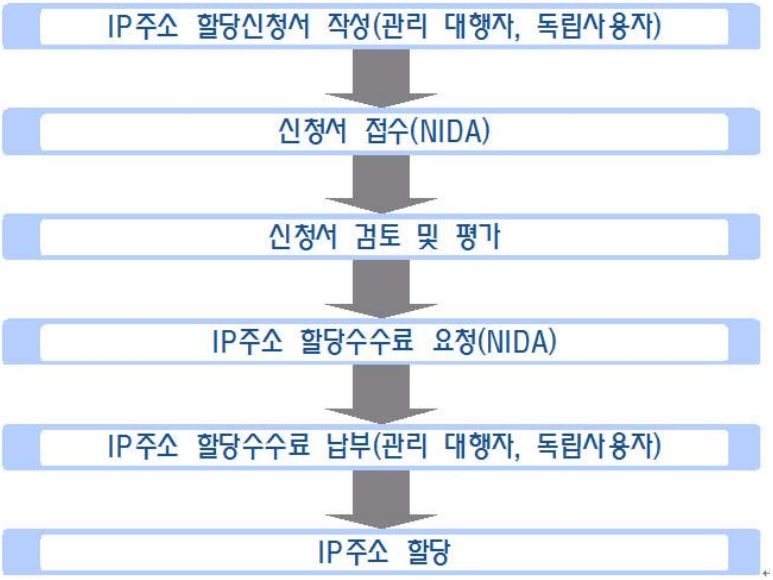
출처 : 한국 첨단망 협회(ANF),

3. IPv6 주소 할당 절차 및 국내 할당 현황

대한민국에서는 한국인터넷진흥원(NIDA)이 APNIC의 NIR로써 국내 인터넷주소자원

을 총괄 관리하고 있다. 〈그림 76〉은 IP주소 할당 절차를 나타내는 그림이고, 〈표 37〉는 IPv6 주소를 할당 받은 국내의 기관 및 주소 현황을 정리한 표이다.

〈그림 76〉 IP 주소 할당 절차



〈표 37〉 국내의 IPv6 주소 현황

구분	기관명	IPv6 주소	LIR 서버	확보일
1	KT기술연구소	2001:0220::/35	KOREN	1999.10.06
2	한국전자통신연구소	2001:0230::/32	ETRI	1999.11.24
3	케이티하이텔	2001:0280::/32	KOLNET	2000.09.27
4	데이콤	2001:0270::/35	DACOM	2000.09.08
5	하나로통신	2001:0290::/32	HANANET	2000.10.30
6	한국통신	2001:02B0::/32	KORNET	2000.09.27
7	한국전산원	2001:0220::/35	6KANET	2001.01.15
8	에스케이텔레콤	2001:02B8::/32	SKSpeedNET	2001.04.06
9	한국과학기술연구원	2001:02D8::/32	KREONet	2001.08.23
10	삼성네트워크스	2001:0320::/32	SAMSUNGGNETW	2001.09.20

			ORKS	
11	두루넷	2001:0230::/32	THRUNET	2001.12.18
12	한국전산원	2001:07FA:0:0002::/64	6KANET	2001.01.15
13	한인터네트워크스	2001:0390::/32	HANINTERNET	2002.02.07
14	㈜케이아이엔엑스	2001:07FA:0:0004::/64	KINX	2002.02.07
15	엔터프라이즈네트워크스	2001:03A8::/32	ENTERPRISENET	2002.04.02
16	드림라인	2001:0C48::/32	DREAMX	2002.08.12
17	케이.알.라인	2001:0C98::/32	KrLine	2002.09.19
18	온세통신	2001:0CF0::/32	SHINBIRO	2003.01.22
19	엔티티코리아	2001:0D38::/32	GIN	2003.05.21
20	케이티프리텔	2001:0E60::/32	KKTFWING	2004.02.13
21	한국교육전산망협의회	2001:0E70::/32	KREN	2004.03.17
22	데이콤-초고속국가망	2001:0E78::/32	PUBNETPLUS	2004.03.17
23	에스케이텔링크	2001:0E98::/32	SKTELINK	2004.03.29
24	㈜관악유선방송국	2001:0EA0::/32	KCNET	2004.03.29
25	㈜케이티네트워크스	2001:0EA8:/32	KITINET	2004.03.31
26	㈜한국무역정보통신	2001:0EB8::/32	KTNET	2004.04.07
27	㈜한국인터넷데이터센터	2001:0ED0::/32	KIDC	2004.04.18
28	반도케이블라인	2001:0EE8::/32	CABLELINE	2004.05.17
29	한국통신-초고속국가망	2001:0EF0:/32	PUBNET	2004.05.24
30	㈜서버뱅크	2001:OEF8::/32	HANNET	2004.05.24
31	에스케이네크웍스	2001:0E28::/32	SKNETWORKS	2004.07.08
32	㈜아이네트호스팅	2001:0E48::/32	INET	2004.08.06
33	한국인터넷진흥회	2001:0DCC::/32	ISP-1	2005.04.27
34	한국통신	2400::/20	KORNET	2005.06.01

4. IPv6 주소 할당 개요

IPv6 는 기본적으로 IPv4의 문제점 중 주소 부족의 문제를 해결하는 것이 주요 목적 중 하나이었던 만큼 풍부한 주소 공간을 가지고 있다. 따라서 IPv6를 정식으로 할당 받은 기관은 IP 주소의 부족 문제는 고민할 필요가 없다고 해도 틀린 말은 아니다. 그러나 단순히 IP 주소가 충분하다고 해서 IP 주소 할당에 아무런 체계나 정책이 필요 없다고 할 수는 없다. IPv6 주소의 체계적인 할당 전략의 필요성을 몇 가지로 요약해 보면 다음과 같다

가. 체계적인 주소 할당 전략의 필요성

1) Renumbering 최소화

IP 노드에 할당된 IP 주소는 하드웨어적으로 고정된 주소가 아니라 IP 라우팅을 위한 식별자로서 논리적인 주소라고 할 수 있다. MAC 주소와 같이 하드웨어적으로 고정되지 않은 논리적인 주소는 상황에 따라 변경될 가능성이 존재하게 된다. 한번 할당된 IP 주소를 네트워크의 변경과 같은 원인으로 인해 다시 설정하는 과정을 IP Renumbering 이라고 한다. IP Renumbering은 네트워크 관리적인 측면에서 시간과 비용의 부담을 발생시키므로 최소화 하는 것이 바람직할 것이다. 체계적이고 합리적인 계획과 정책에 따른 IP 주소 할당 전략은 시간과 비용의 부담을 발생시키는 IP Renumbering 발생 가능성을 최소화 하는데 기여 할 수 있다.

2) 주소 낭비의 최소화

위에서 언급한 바와 같이 IPv6 주소는 Prefix /64의 단일 Subnet에 264개의 IP 주소를 할당 할 수 있을 정도로 매우 큰 주소 공간을 가지고 있다. 이렇게 충분한 주소를 가지고 있다고 하더라도 체계와 기준이 없는 IP 주소 할당은 필연적으로 IP 주소의 불필요한 낭비를 초래하게 되고 이는 결코 바람직한 것은 아니다. 체계적이고 합리적인 IP 주소 할당 정책을 통해 IP 주소의 낭비를 최소화 할 수 있다.

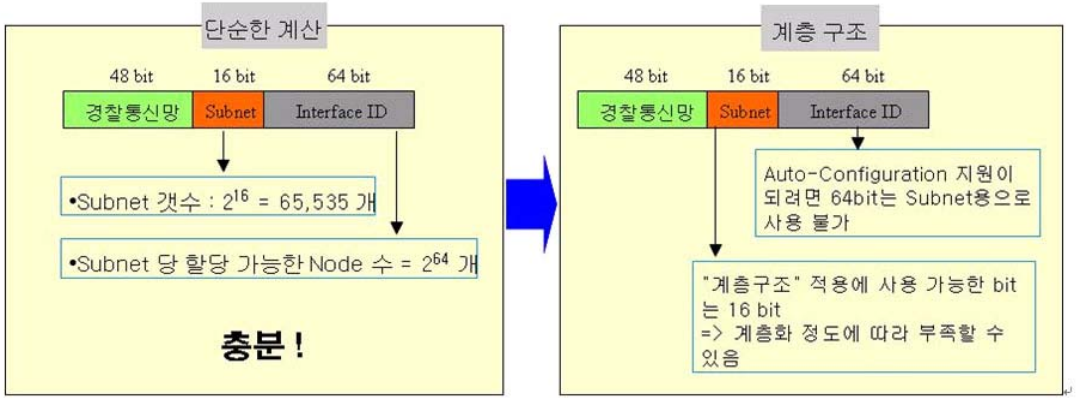
3) 관리 비용 절감

체계적이고 합리적이며 계획에 맞게 할당된 IP 주소는 할당, 회수, 재분배 그리고 장애 처리 등의 관리적인 측면에서 효율성을 높일 수 있다.

4) IP 주소의 계층화에 따른 관점

위에서 IPv6의 주소는 충분하다고 하였지만, 이는 Subnet당 할당 가능한 IP 노드수를 계산한 단순한 결과일 뿐이다. 실제 IP 네트워크의 설계에 대해 생각해 본다면 라우팅의 효율성 등을 높이기 위하여 "계층화된" 설계가 필요하다. 이를 위해서는 Subnet을 단순히 순차적으로 할당하는 것을 지양하고 계층화 구조를 갖도록 해야 한다. 또한 IPv6의 큰 장점 중 하나인 Auto-Configuration을 활용하기 위해서는 IPv6 주소 128 bit 중 하위 64 bit는 호스트(IP 노드)의 MAC 주소를 삽입하기 위한 공간으로 예약된 것으로 봐야 한다. 예를 들어 Prefix /48 IPv6 주소 블록을 할당받은 기관의 경우 〈그림 77〉을 보면 계층화된 Subnet을 위해 사용 가능한 bit 는 16bit 에 불과 하다. 16bit 는 계층화의 정도에 따라 충분하지 않을 수도 있으며 따라서 필요한 계층화의 정도, 각 계층에 필요한 Subnet의 개수 등을 정확히 파악 하고 정확한 데이터에 의한 체계적이고 합리적인 IP 주소 할당 정책 도출이 필요하다.

〈그림 77〉 계층화 구조를 갖기 위한 IPv6 주소 공간 계산



나. 관련 IETF 작업 문서

IPv4, IPv6의 주소 할당과 관련된 대표적인 인터넷 관련 표준화 기구들의 작업 결과를 요약해 보면 다음과 같다

1) RFC 3177

TCP/IP에 관련된 대표적인 표준화 단체인 IETF의 상위기관인 IAB(Internet Architecture Board)와 IAB의 하위 기관 중 IESG(Internet Engineering Steering Group)에서 IPv4, IPv6 에 대한 주소 할당과 관련된 기본적인 제안을 하였는데 요 약하면 다음과 같다(RIRs-on-48로 표현).

- 일반적인 경우
  . /48 : 가장 일반적인 경우에 할당, 단 매우 큰 가입기관은 예외
  . /64 : 오직 하나의 Subnet만 필요한 가입기관에 할당
  . /128 : 오직 하나의 device에 할당
- 특별한 경우
  . Home 네트워크 사용자, On-Demand 혹은 Always-On 연결 사용자에게는 /48 할당
  . 소규모, 혹은 대규모 Enterprise 에게 /48 할당
  . 매우 큰(very large) 규모의 가입기관은 /47 혹은 약간 작은(주소 규모로는 커짐) Prefix, 또는 여러 개의 /48 Prefix 할당

1) RFC 1219

IPv4 주소 블록에서 bit수를 관리하는 효율적인 방법 제안

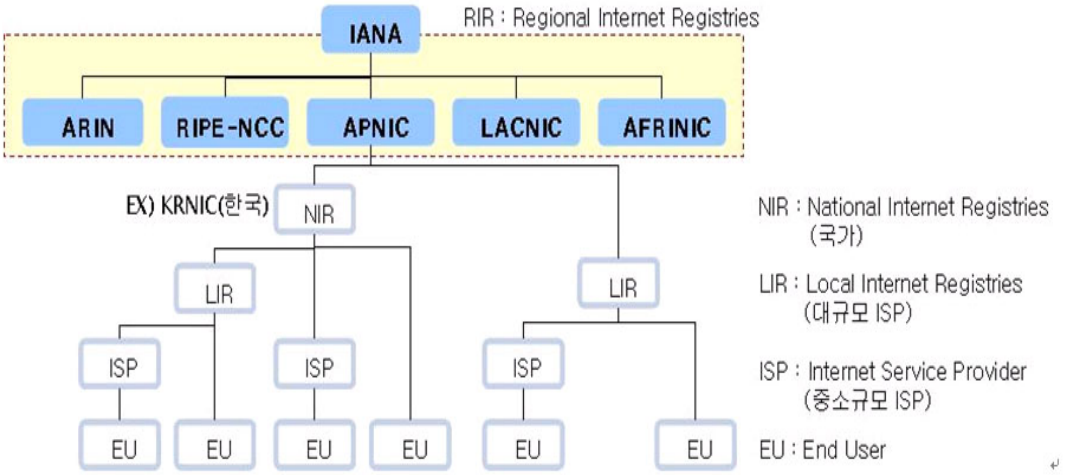
2) RFC 3531

RFC 1219를 IPv6 주소에 적용

다. 전 세계 인터넷 주소 관리체계

위에서 언급한 IAB 산하 IANA(Internet Assigned Numbers Authority)에서 IP 주소를 총괄 관리한다. IANA 하위에는 대략 대륙별로 별도의 관리 기구를 두었고 그 하위에 각 국가별 관리 기구(NIR)가 존재한다〈그림 78〉. 한국은 APNIC 산하 NIDA(한국인터넷진흥원)에서 IP 주소의 총괄 관리를 담당하고 있다. NIDA 하위에는 대규모 ISP라고 할 수 있는 LIR이 있고(한국의 경우 KT 등) LIR 하위에 중소규모 ISP 라고 할 수 있는 ISP들이 있으며 최종적으로 IP 주소를 할당 받는 기관은 EU로 표현한다. EU는 기관의 규모에 따라 LIR에게 직접 IP 주소를 할당 받을 수도 있으며 ISP를 통해서 받을 수도 있다. 경찰청의 경우 규모로 볼 때 LIR에서 할당 받을 것으로 예상된다.

〈그림 78〉 전 세계 인터넷 주소 관리 체계도



또한 세계 각국의 IPv6 주소 확보 현황을 〈표 38〉에 정리 하였다. 한국은 독일, 일본, 유럽에 이어 확보량 4위를 기록하고 있으며 Prefix /32 블록 4,145 개에 해당한다.

〈표 38〉 국가별 IPv6 주소 확보 양

순 위	국 가 명	IPv6수(/32)	순 위	국 가 명	IPv6수(/32)
1	독일	9,305	8	미국	146
2	일본	7,270	9	영국	85
3	유럽연합	6,159	10	스위스	54
4	대한민국	4,145	11	이탈리아	31
5	호주	4,106	12	프랑스	29
6	네덜란드	560	13	오스트리아	24
7	노르웨이	266	14	기타	363

라. 국내 IPv6 주소 할당 정책

위에서 언급한 바와 같이 국내 IP 주소 관리는 한국인터넷진흥원(NIDA)에서 총괄하고 있다. NIDA의 IP 주소 정책 관련 문서에서 IPv6에 관한 정책을 요약하면 다음과 같다.

1) 할당 주소 공간 크기

- IPv6 주소 공간의 할당은 기존의 RFC3177과 RIRs-on-48의 지침에 의거하여 실시함
- 아주 큰 가입 기관을 제외하고 일반적으로 /48 할당

2) 단일 Site에 대한 복수개의 /48 할당

- 단일한 Site가 추가적인 /48 주소 블록 요청 시 주소가 추가로 필요하다는 증빙 문서나 증빙 할 수 있는 자료를 제출하여야 함
- 복수개 또는 추가적인 /48 신청은 APNIC/NIDA 차원에서 진행되고 검토될 것임 (예: 정당성 검토)
- 동일한 Site에 대하여 복수개의 /48 할당의 경험은 현재(2002.7.2일 기준)는 없으며 APNIC은 경험을 통하여 공통의 정책이 개발될 때까지 그러한 할당을 일시적인

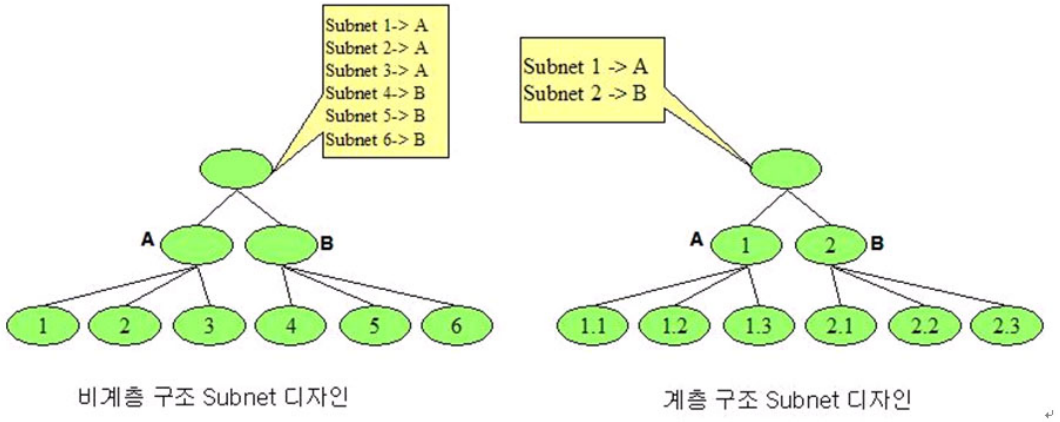
방편으로 검토할 것임

이상에서 보는 바와 같이 NIDA의 IPv6 주소 할당 정책이 위에서 살펴본 국제기구의 정책과 크게 다르지 않다는 것을 알 수 있다. 중요한 것은, 경찰통신망에서 필요한 IPv6 주소 블록이 /48 로서 충분하다면 문제가 없겠으나 /48 이상이 필요하다고 한다면 /48 이상의 주소 블록을 요청해야 할 것이며 이를 위해서는 /48 이상이 필요하다는 타당성을 증명해야 할 자료를 제시해야 한다.

마. 계층적인 Subnet 구조

IP 네트워크를 설계할 때 각 Subnet을 계층적인 구조로 설계하는 것이 라우팅 효율적인 측면이나 관리 적인 측면에서 장점이 있다.

〈그림 79〉 계층 구조 Subnet과 비계층 구조 Subnet의 비교



〈그림 79〉에서 보면 계층 구조를 갖지 않는 Subnet의 경우 최상위 스위치 장비는 하위 6개의 Subnet에 대한 라우팅 정보를 6개 모두 가지고 있어야 하는 반면 계층 구조를 갖는 경우에는 2개의 라우팅 정보만 가지고 있어도 된다. Subnet의 개수가 많아지고 대규모 네트워크일수록 이 점은 큰 비교 포인트가 된다.

5. IPT 규격 비교(NIA vs. 행정자치부)

◎ 호 처리 및 연동 방식 기능 규격

구분	기능 요소		기능 설명
	NIA	행정자치부	
호 처리	-	이중화 호 처리 (필수)	시스템 이중화로 시스템 장애 발생에 대한 호 처리에 문제가 없어야 함 Active/Standby 이중화 구조를 통해 호 처리
	-	로드밸런싱 (필수)	• 하드웨어적인 이중화 구조 지원 • 하드웨어 및 소프트웨어 측면에서 실시간 이중화 운용 지원
	-	호 처리 수용용량(권고)	• 시/도 IPT 제원 : 30,000 이상 가입자 수용 • 시군구 IPT 제원 : 5,000 이상 가입자 수용
연동 방식 기준	IPv4-IPv6 간 연계	-	NAT-PT를 활용하여 IPv4와 IPv6 간의 주소 변환 지원
	-	IP망 연계 (필수)	• IP망과 연동을 위한 Fast Ethernet (TX or FX) 인터페이스를 2개 이상 제공 • 고정 IP와 유동 IP 모두 지원 • CAC (Call Admission Control) IP망을 경유한 불법 접근을 차단하기 위한 ACL (Access List)을 설정할 수 있어야 한다. • 음성패킷 QoS를 위하여 DSCP Write 기능이 지원 • 내부 IP망 연동 ACL 기능 지원 • 음성과 데이터 트래픽에 대해서 음성 트래픽을 우선 처리할 수 있는 QoS 기능 지원
	VoIP망과 PSTN 연동	VoIP망과 PSTN 연동 (필수)	• 일반전화기 연동을 위한 FXS 인터페이스 제공 • 전화교환기 연동을 위한 FXO, PRI, CAS 또는 R2 인터페이스 제공 • Access Gateway를 통한 연동 지원

◎ 품질 기준 및 운용관리 기능 규격

구분	요소		설명 (품질 기준)
	NIA	행정자치부	
IP 단말 품질 기준	단대단 지연	Delay (선택)	단방향 150ms 이내
	R 값	-	R값 70 이상
	-	통화품질 (선택)	• G.729 코덱 사용시 R값 70 이상 (MOS 3.6) • G.711 코덱 사용시 R값 80 이상 (MOS 4.0)
	호 성공률	호 성공률 (선택)	95% 이상
운용관리 기능	-	시스템 관리 및 모니터링 (필수)	시스템의 각 구성장비에 대한 관리 및 모니터링 기능 제공을 위한 모듈 제공
	-	Reporting (필수)	시스템 장애 발생시 실시간으로 리포팅이 되어야 하며 각 장비별 내역조회가 가능
	-	성능 관리 (필수)	시스템의 각 구성장비에 대한 성능분석 및 실시간 성능 모니터링 기능 제공
	-	원격 구성관리 (필수)	• 원격 구성관리를 위해서 Telnet (CLI) 또는 Web Client를 제공 • 네트워크 단절 등의 문제 발생시 접속할 수 있는 콘솔모드를 제공
	-	구성정보 관리 (필수)	• IP 주소 및 번호 등을 확인하기 위한 기능 제공 • 시스템 구성정보를 주기적으로 백업하는 기능 제공
	-	보안관리 (필수)	• 시스템은 운용자의 등록, 변경 및 삭제가 가능 • 운용 등급 관리가 가능
	-	장애관리 (필수)	장애감시 및 통보, 장애 표시, 장애 이력관리, NMS 연동 기능 제공
	-	호 통계 및 모니터링	시스템에서 발생되는 트래픽에 대한 통계기능을 제공

6. IPT 장비 규격 예시 및 견적가

◎ IP-PBX 규격

구분	요구 규격 및 주요 기능		중요도	비고
일반 사항	• 운영체제는 안정성이 보장되어야 함. (Open Source 기반의 Linux 및 상용 Unix/Windows 등) • 소프트웨어 라이센스를 통한 가입자 증설 기능 제공		필수	
표준 프로토콜	신호 프로토콜	• TTA 및 IETF에서 규정한 SIP (IPv6 지원) 사용	필수	
		• H.323	선택	
	IP 프로토콜	• IPv4, IPv6, SNMP, RTP 지원	필수	
	Fax 서비스	• T.38 Fax Relay	필수	
음성/영상 코덱 기술	음성 코덱 (ITU-T 표준)	• G.711	필수	
		• G.729A, G.723.1, G.722 지원	선택	
	영상 코덱 (BcN 채택)	• H.263	필수	
		• H.264, MPEG4 지원	선택	
	영상서비스 해상도	• CIF, QCIF	필수	
인터페이스	Analog I/F	• FXS/FXO 4 Port 이상 지원	필수	
	Digital I/F	• E1 1Port 이상 지원	필수	
	LAN I/F	• Fast Ethernet 1 Port 이상 지원 • 향후 Gigabit Ethernet 1 Port 이상 지원 가능	필수	
시스템 관리기능	• SNMP, Web을 통한 상태정보 및 업그레이드 관리 기능 지원 • 사용자 및 관리자의 편이성 제공을 위한 Web 모델 서비스 기능 • GUI를 이용한 시스템 관리 기능 • 실시간 성능/장애/호통계/보안 정보에 대한 모니터링 기능, 상세 내역조회/리포팅 기능 • SNMP를 통한 시스템 관리 기능		필수	
호처리 기능 (서버)	일반 사항	• Call Admission Control 을 이용한 호 제어 기능 • 관리자의 편리한 서비스 관리를 위한 그룹핑 기능 (User/TEANT Group 등) • WAN 구간 장애시 우회경로 자동 전환 및 PSTN으로 호를 우회시키는 기능 • SIP와 H.323 프로토콜간 Signaling Interworking 기능 • 내/외선 호에 대한 멜소리 구분 기능 • 호처리 및 음성 회선에 대한 암호화 기능 (sRTP, TLS, IPSec) • Inband 또는 Out-of-Band 방식의 DTMF Relay 기능 • T.38 Real-Time Fax, Pass-Through 방식의 Fax 기능 • 방화벽 및 사설 IP 환경에서의 인터넷전화서비스가 가능하도록 하는 NAT/FW Free Solution 기능	필수	
	Call Control 및 Routing 기능	• Internal Call Control • Inbound/Outbound Call Control • Prefix Based Number Plan • Address/Number Translation • Call Routing • Direct Inward/Outward Dialing • Auto Network Dialing	필수	
시스템 최대 용량	• 15,000명 이상 가입자 수용 가능 • 65,000 BHCA 이상 처리 가능 • IP 단말 내선 : 15,000 회선 이상 • User Group 최소 100개 이상 지원		필수	

구분	요구 규격 및 주요 기능		중요도	비고
Redundancy	• Active-Active 또는 Active-Standby 방식의 이중화 구조 지원		필수	
음성 품질	단대단 지연	• 단방향 150ms 이내	필수	
	R값과 MOS	• G.729 코덱 사용시 R값 70 (MOS 3.6) 이상 • G.711 코덱 사용시 R값 80 (MOS 4.0) 이상		
	호 성공률	• 95% 이상의 호 성공률 지원		
연동 및 호환 기능	• 통신사업자의 소프트스위치 및 게이트키퍼 시스템과의 연동 기능 지원 • 기존에 설치된 PBX 교환기 및 키폰 시스템과의 연동 기능 지원 • 기존 아날로그 전화기를 수용하기 위한 연동 기능 지원 • 다양한 벤더의 IP 교환기 시스템과의 연동 기능 지원 • 다양한 벤더의 IP 전화기 및 Gateway와의 연동 기능 지원 • PSTN과의 연동 기능 (PRI, R2 등의 인터페이스 기능) 지원 • 단일 또는 다수의 통신사업자 시스템과의 동시 연동 기능 지원 • 향후 민원센터/콜센터 구축시 고객센터용 교환기와의 연동 기능 지원		필수	
	• IPv4-IPv6간 주소 변환 기능 지원		선택	
보안	• 신호 정보보호	• HTTP 인증, IPSEc/TLS, S/MIME 등의 보안기술 적용을 통한 트래픽 암호화 기능		
	• 음성/영상 정보보호	• 공중 인터넷망 구간 트래픽 전달시 음성/영상 트래픽에 대한 암호화 기능 • sRTP 등을 활용한 미디어 트래픽에 대한 암호화 기능		

◎ Voice Gateway 규격

구분	요구 규격 및 주요 기능		중요도	비고
일반 사항	• 시스템 신뢰성 확보를 위해 주교환기 (IP-PBX) 장애 시, 자체 로컬 호처리 기능 제공		필수	
표준 프로토콜	신호 프로토콜	• TTA 및 IETF에서 규정한 SIP (IPv6 지원) 사용	필수	
		• H.323	선택	
	IP 프로토콜	• IPv4, IPv6, SNMP, RTP 지원	필수	
	Fax 서비스	• T.38 Fax Relay	필수	
음성/영상 코덱 기술	음성 코덱 (ITU-T 표준)	• G.711	필수	
		• G.729A, G.723.1 지원	선택	
	영상 코덱 (BcN 채택)	• H.263	필수	
		• H.264, MPEG4 지원	선택	
	영상서비스 해상도	• CIF, QCIF	필수	
인터페이스	Analog I/F	• FXS/FXO 4 Port 이상 지원	필수	
	Digital I/F	• E1 1Port 이상 지원	필수	
	LAN I/F	• Fast Ethernet 1 Port 이상 지원 • 향후 Gigabit Ethernet 1 Port 이상 지원 가능	필수	
시스템 관리기능	• GUI를 이용한 시스템 관리 기능 • 실시간 Alarm 발생 및 검색 기능 • 실시간 Trace 및 Message 통계 기능 • CLI, Telent, SNMP를 통한 시스템 관리 기능		필수	
호처리 기능 (서버)	• E.168 에코 제거 및 128ms의 Echo Tail Length 기능 지원 • 음성 활동 탐지(VAD), 잡음 억제 (SCE), 컴포트 노이즈 (CNG) 기능 지원 • QoS 기능 (802.1p/q, DSCP) 지원 • 발신자 ID (Caller-ID) 표시 기능 지원 • T.38 Real-Time Fax, Pass-Through 방식의 Fax 기능 지원 • 운용 중, Hot-Swap 방식의 카드 교체 기능 지원 • 통화 진행 중 톤 탐지 및 생성 : 다이얼톤, 통화중톤, 통화대기음, 복주/재시도톤		필수	
시스템 최대 용량	• 100명 이상 가입자 수용 가능 (주교환기 장애 시 가입자 수용용량) • 500 BHCA 이상 처리 가능 • Digital Trunk : E1 1ghltjs (30CH) 이상 지원 • Analog Trunk : 10회선 이상 지원 • IP 단말 내선 : 100회선 이상 지원 • 일반내선 : 10회선 이상 지원 • 디지털내선 : 30회선 이상 지원		필수	
보안	• HTTP 인증, IPSEc/TLS, S/MIME 및 sRTP 등의 보안기술 적용을 통한 트래픽 암호화 기능			

◎ IP Phon 규격

구분	요구 규격 및 주요 기능		중요도	비고
일반 사항	• 하나 이상의 호가 대기중일 때, 전화기의 램프 또는 LCD 창을 통해 표시되는 기능 • 회의 통화 및 구성 기능, 화상 전화 기능 • 전화번호 검색 기능, 볼륨 조절 기능 • 동시에 3개 이상의 전화를 받을 수 있는 기능 • Automatic 802.1q VLAN 기능, DiffServ (TOS) 및 802.1p 기능 • CID, 송수신 번호 및 이력 사항, Call 상태, 부재중전화 상태 확인 기능 • E.168 에코 제어, VAD, CNG, Dynamic Jitter Buffer, Silence Suppression 기능 • DTMF Detection, DTMF Inbound/Outbound Relay 기능 • Distinctive Ringing : 내/외선별 별도의 벨소리 제공 기능 • 신호 및 음성/영상 트래픽에 대한 암호화 기능		필수	
표준 프로토콜	신호 프로토콜	• TTA 및 IETF에서 규정한 SIP (IPv6 지원) 사용	필수	
	IP 프로토콜	• IPv4, IPv6, SNMP, RTP 지원	필수	
음성/영상 코덱 기술	음성 코덱 (ITU-T 표준)	• G.711 a/u-law	필수	
		• G.729A/B, G.723.1 지원	선택	
	영상 코덱 (BcN 채택)	• H.263	필수	
		• H.264, MPEG4 지원	선택	
	영상서비스 해상도	• CIF, QCIF	필수	
인터페이스	• 2개의 10/100 스위치 포트 제공		필수	
시스템 관리기능	• Web 을 통한 IP 전화기 정보 구성 • FTP/TFTP 등을 이용한 원격 소프트웨어 업그레이드 기능 • PoE 기능		필수	

◎ Soft-Phon 규격

구분	요구 규격 및 주요 기능		중요도	비고
일반 사항	• 아이디, 패스워크를 이용한 로그인/로그아웃 기능 • 초기 메시지 표시 기능 • 일반정보, 서버정보, 사용자정보, 음성정보, 영상정보에 대한 설정 기능 • SIP Inbound/Outbound 처리 기능 • 통화중 Mute, Call Hold 기능 • 다중 코덱 협상 기능 • 음성, 영상 통화 기능 • DTMF 처리 기능 • Pulg&Play 기능 • 시스템으로부터의 자동 업그레이드 기능 • 착신 거부, 대리 응답, 3자 통화, 회의 통화 기능 • 발/착신 통화 기록, 통화 이력 사항에 대한 발/착신 호출 기능 • 대체 이미지 전송 기능 • 신호 및 음성/영상 트래픽에 대한 암호화 기능		필수	
표준 프로토콜	신호 프로토콜	• TTA 및 IETF에서 규정한 SIP (IPv6 지원) 사용	필수	
	IP 프로토콜	• IPv4, IPv6, RTP 지원	필수	
음성/영상 코덱 기술	음성 코덱 (ITU-T 표준)	• G.711 a/u-law	필수	
		• G.729A/B, G.723.1 지원	선택	
	영상 코덱 (BcN 채택)	• H.263	필수	
		• H.264, MPEG4 지원	선택	
	영상서비스 해상도	• CIF, QCIF	필수	

◎ VMS 규격

구분	요구 규격 및 주요 기능	중요도	비고
일반 사항	• 음성 멘트 관리 기능 • 메일박스 2000 유저 이상의 지원 • IP-PBX 연동 기능 • 메시지 알림 및 사서함 자동 등록 기능 • 내부 또는 외부에서 전화기를 통한 간편한 녹음 기능 • 개별 사서함 환경 설정 기능 • 메시지 녹음, 전화번호 남김, 안내원 연결, 메시지 전달 및 메시지 확인 기능	필수	

◎ MCU 시스템 규격

구분	요구 규격 및 주요 기능	중요도	비고
일반 사항	• 음성 세션과 영상 세션의 믹싱 기능 • Announcement Play 기능 및 녹화 기능 • 최대 16명 이상의 회의 참석 기능 • 웹에서의 회의 즉시 개시 및 특정 시간에 회의를 개시할 수 있는 예약 기능 및 변경 기능 • 진행 중인 회의 제어·관리 기능 : 녹화/녹취, 참가자 강제퇴장/재호출, 발언권 제어, 추가 호출, 회의 종료 • 종료된 회의에 대한 회의 정보 조회 기능 • 각 개인별 주소록 생성/변경/삭제 기능	필수	

◎ 그룹웨이/전자결제 시스템 규격

구분	요구 규격 및 주요 기능	중요도	비고
일반 사항	• IP-PBX 연동 기능 • 그룹웨어 및 전자결재를 위한 Click-to-Call 기능 • 전자결재, 메일, 메신저의 개인 주소록 연계를 통한 일정관리 기능 • 카페 게시판 기능 및 웹하드 기능 • 업무 진행 상황의 실시간 보고를 위한 알리미 기능	필수	

◎ IM/Presence 규격

구분	요구 규격 및 주요 기능	중요도	비고
일반 사항	• IP-PBX 연동 기능 • 메신저를 통한 Click-to-Call 기능 • 등록 상태자 정보 생성/변경/삭제 기능 • 클릭투콜, 인스턴스 메시징 서비스 및 컨퍼런스 서비스 연계 기능 • VMS 서버 및 메일링 서버와의 연계 기능 • 파일 전송 기능 • 등록 상대자의 상태 정보 변경시 이벤트 알림 기능 • 메시지 알림 기능	필수	

위의 IPT 장비의 규격을 바탕으로 시스템 구성 시 각 벤더별 견적가 비교는 다음과 같다.

◎ 장비벤더 견적가 비교

구분		소요 물량 (식)	해외 벤더		국내 벤더		비고
			Cisco	Avaya	LG-Nortel	Xener	
IP-PBX		2	18.7억원	14.5억원	30.1억원	15.6억원	1Site 이중화 구성
게이트웨이		11	0.9억원	-	5.2억원	1.1억원	
IP Phone	IP 전화기	12,750	23.7억원	38.2억원	54.7억원	18.0억원	
	무선 IP 전화기	2,250	10.1억원	6.7억원	17.2억원	6.2억원	
PoE 스위치		625	13.6억원	9.3억원	14.4억원	11.7억원	
IM/PS 서버		1	17.4억원	1억원	-	2.0억원	
VMS 서버		1	0.7억원	5.2억원	-	2.2억원	
MCU 서버		1	1.4억원	3.2억원	-		
그룹웨어/전자결재 서버		1	-	1억원	-	2.2억원	
특이 사항			부가세 포함	IM/PS 및 그룹웨어 서버는 기존 시스템과의 연동기능 개발 비용	부가세 별도	VMS/MCU 기능을 동시 지원하는 장비 제안, 부가세 별도	
제안가격			**95.3억원**	**79.1억원**	**121.6억원**	**59억원**	부가세 일괄 적용

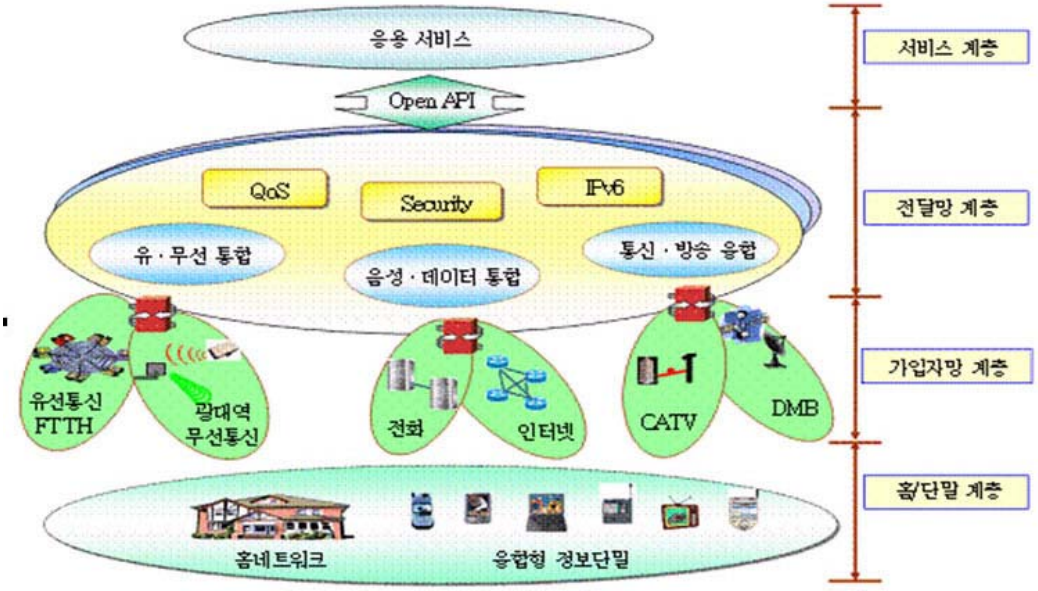
7. BcN

가. BcN 개요

광대역 통합망(BcN)이란 통신, 방송, 인터넷이 융합된 품질보장형 광대역 멀티미디어 서비스를 언제, 어디서나, 끊김없이(seamless) 안전하게 광대역으로 이용할 수 있는 차세대 통합 네트워크를 말한다.

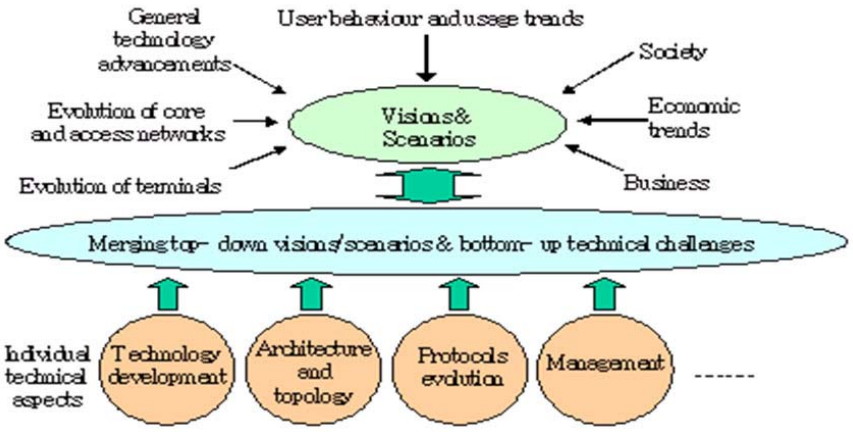
즉, 다양한 서비스를 용이하게 제공할 수 있는 개방형 플랫폼(Open API) 기반의 통신망과 네트워크 단말에 구애 받지 않고 다양한 서비스를 끊김없이 이용할 수 있는 유비쿼터스 서비스 환경을 지원하는 통신망이다.

〈그림 80〉 BcN 구성 개념도



BcN의 의미를 살펴보면 수 십년간 이어 오던 텔레콤 망이 데이터 기반 유선 인터넷뿐만 아니라 3G/4G 및 무선 인터넷이 결합하여 Network Convergence 및 Service Convergence를 통하여 새로운 수익 모델을 창출하기 위함이다. 또한 기존 망 사업자는 음성 전화의 cash cow가 사라지고 있는 상황에서 고품질의 융합 서비스를 통한 신규 수익을 창출할 수 있는 망으로써 BcN을 고려하고 있다. 특히, 정보화 사회가 진화됨에 따라 기존 산업 사회의 비즈니스보다는 사이버 네트워크 상의 멀티미디어 비즈니스가 훨씬 많은 수익을 가져다 줄 것으로 예상하여, 정보통신망을 활용한 사이버 시장을 보다 적극적으로 발굴하기 위한 노력의 일환이다. 즉, BcN의 전략적인 개념은 〈그림 81〉에서와 같이 기존의 ISDN/B-ISDN 등과 같이 기술 개발 측면에서 출발한 것이 아니라 정보화 사회의 새로운 사이버 시장을 창출하고자 하는 비즈니스 및 사회적인 측면에서 출발한 것이다.

〈그림 81〉 BcN 전략적인 비젼 및 시나리오



이러한 정보통신 산업 전략에 따라 정부는 통신사업자들이 미래를 걸게 할 새로운 성장 동력원으로 BcN을 제시했다. BcN은 기존에 음성전화시장으로 상징되어 온 기존의 통신 시장 구도를 유무선 통합, 통신과 방송 융합 등 새로운 컨버전스 시대로 전환하게 될 것이다. 이를 통하여 2010년까지 유선과 무선에서 각각 50Mbps급 이상의 광대역 통신망을 구축하고 다양한 컨버전스형 서비스를 확산시키겠다는게 정부의 BcN 전략이다.

나. BcN 기술 개요

1) BcN 기술의 주요 개념 및 특징

광대역 통합망은 궁극적으로 사람들이 거주하는 모든 가정 및 사무실에 광대역으로 네트워크 접속을 허용하고, 이동 중이거나 고정된 상태이거나 관계없이 항상 네트워크 접속이 가능하게 하는 것이다. 나아가 네트워크에 접속되어 있는 자신이 소유하고 있는 장비를 네트워크를 통하여 제어하는 것이 가능하게 하는 것이다.

이러한 광대역 통합 서비스 개념은 모든 형태의 정보통신 서비스에 대한 지원이 가능하고, 네트워크 인터페이스에 대하여 개방되고 공정하게 이용할 수 있도록 하며, 각기 다른 네트워크에 대하여 공통의 구조를 채택하여 이를 통합할 수 있도록 한다. 또한 기존 서비스뿐만 아니라 신규 서비스에 대하여 어떤 시간이나 어떤 장소에서나 멀티미디어 서비스

를 제공 가능하게 하는 것을 목표로 한다.

광대역 통합 서비스를 위한 단말 사용자 요구사항을 보면, 첫째로 어떠한 제약이 없이 중단 없이 서비스가 가능하게 되어야 하며, 둘째로 유선이든 무선이든 관계없이 통합 단말기를 용이하게 사용할 수 있어야 한다. 셋째로 동일한 번호 계획과 네이밍 시스템을 사용해야 하며, 넷째로 서비스 등급에 따라 차등적인 과금이 가능해야 한다.

한편 광대역 통합 서비스를 위한 망 공급자 요구사항을 보면 서로 다른 망 사업자 간에 자원 효율을 높일 수 있도록 경제적인 투자가 이루어져야 하며, 서비스와 망 장비간에 개방형 인터페이스 플랫폼을 제공하여 서비스 제공 비용을 최적화해야 한다. 또한 망 사업자 간에 통합 과금 시스템을 도입하여 상호 정산을 위한 부가적인 부담을 줄이고, 중단 없는 서비스를 위하여 이동성이나 로밍 서비스를 지원해야 한다.

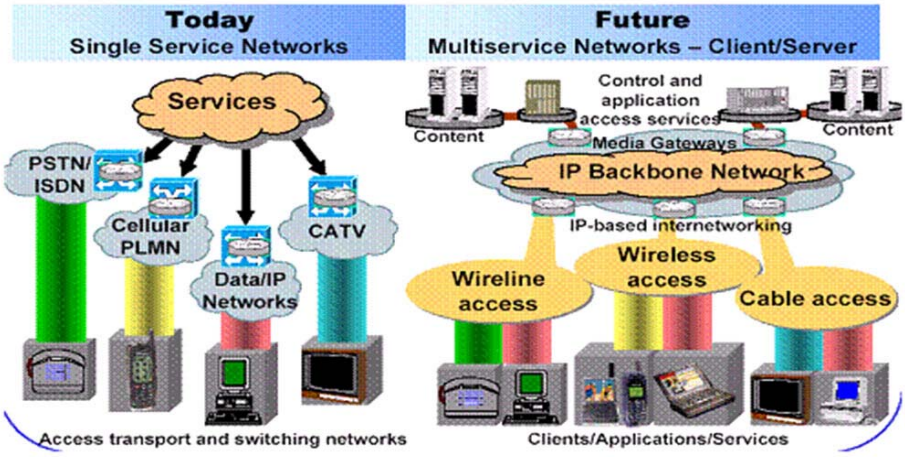
여기서 특이 사항은 향후 정보통신 서비스는 플랫폼 개념이 개방형 인터페이스(Open API: Application Program Interface)를 가장 중요한 항목으로 취급을 하는 데 이는 망 구조와 기능 구성에 있어 개방적이고 경쟁력이 있는 환경을 제공할 수 있기 때문이다. 또한 Open API는 새로운 신규 서비스를 개발하는 환경에 가장 효과적인 인터페이스라고 판단하고 있다. 또한 BcN 이 향후에 등장할 모든 형태의 정보통신 서비스를 수용할 것을 가정한다면 전화에서부터 멀티미디어에 이르기까지 모든 서비스 유형뿐만 아니라 실시간, 차등적인 서비스 품질, 일대일 및 일대다중 연결 등과 같은 다양한 전송 특성을 제공해야 한다. 이와 같이 다양한 정보통신 서비스를 위하여 BcN 에서는 서비스를 네트워크로부터 분리하려는 개념이 강하게 등장을 하는 데 이는 즉, 서비스 기능을 전달 능력으로부터 분리를 시키고, 서비스는 망 하부구조에 관계없이 그 자체 진화적인 요소로 도입이 되어야 할 것으로 분석되고 있다.

2) BcN 기술 발전 전망

현재 네트워크 환경을 보면 기존의 전통적인 전화망과 사설 전용선망, 위성방송망, 케이블망 및 무선/이동 통신망을 비롯하여 최근 인터넷까지 다양한 형태의 망이 공존하고 있다. 최근의 인터넷과 무선/이동 통신망이 급속히 확대됨에 따라 기존 개별 통신망과 융합하려는 BcN의 탄생은 어쩌면 당연한 것으로 생각된다. 광대역통합망이 완성이 되면 일

반 가입자는 자신이 소유하고 있는 단말기 형태에 무관하고, 유선이든 무선이든 접속된 망에 관계없이 언제 어디서나 자유롭게 대화하고 필요한 정보를 원하는 품질로 얻을 수 있을 것이다.

〈그림 82〉 멀티 서비스 통합망으로 망 구조 전환 개념



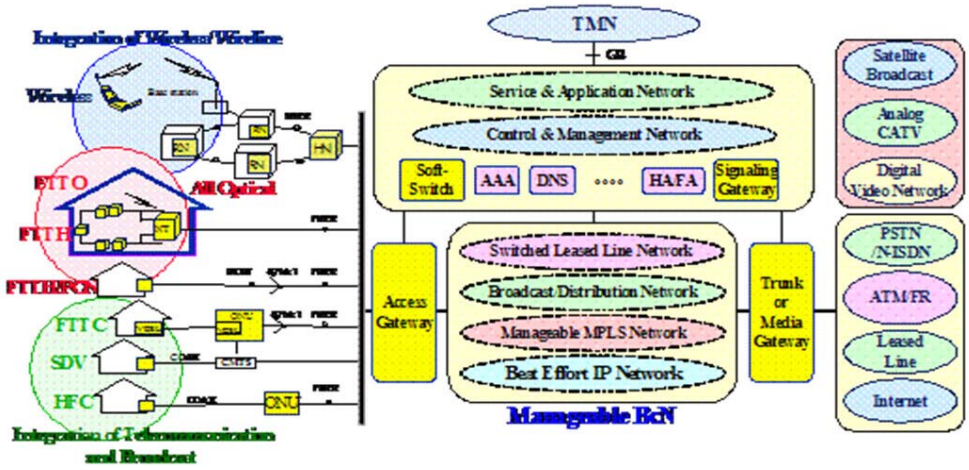
BcN에서 품질보장 서비스가 제공되면 사용자가 원할 때 99.999 % 가용도(이는 1 년에 접속 불량 시간이 10 분 이하인 경우임)를 가지고 항상 망에 접속할 수 있으며, 내가 원하는 데이터, 음성 및 영상 정보를 내가 원하는 시간 이내에 다양한 품질로 받을 수 있다. 또한, 보안 측면에서 정보의 유출을 걱정하지 않고 마음 놓고 은행 업무도 볼 수 있는 여건이 조성된다. 이는 모든 개인과 회사의 비즈니스 업무에서 공기나 물과 같이 가장 필요로 하는 신뢰하는 네트워크 환경이 구축되게 된다.

현재 유선 또는 무선 인터넷은 급속히 보급되고는 있으나 종단간의 서비스 품질을 보장을 해주지 못해서 새로운 정보통신 비즈니스의 걸림돌이 되고 있다. 이는 현 인터넷이 네트워크 이용을 위해 사전 예약하는 기능이 없고 현재 가용한 리소스 상태에서만 상호 접속이 가능하기 때문이다. 인터넷 연구그룹에서 검토하고 있는 Diffserv 서비스 또는 Intserv 서비스 모델은 실질적으로 망에서 운용이 곤란하다. 왜냐하면 차별화된 우선 순위를 주거나 대역을 보장하기 위해서는 이에 상응하는 요금을 받으면서 이를 운용하고 감

시할 수단이 있어야 하는데 이를 위한 마땅한 수단이 없기 때문이다. 또한 현재 가장 시급히 요구되고 있는 정보 보안 능력도 가입자 단말 서비스간에는 가능하나 네트워크 측면의 적절한 보안 능력을 제공하는 것은 현 인터넷 구조에서는 매우 어렵다.

따라서 통신망 사업자 측면에서 기존 인터넷 망은 서비스 품질을 제어할 수가 없어서 엄청난 시설 투자에도 불구하고 가입자로부터 품질 불만을 사고 있는 실정이다. 더구나 현 인터넷이 데이터중심으로 설계되어 점차적으로 대용량의 파일이나 음성, 영상 및 방송 트래픽을 전달하는 데는 많은 기능의 보강이 요구되고 있다.

〈그림 83〉 BcN 망 구조 개념



광대역통합망의 트래픽 엔지니어링 기술은 기존 전화망 또는 인터넷, 무선망과 차별화시킬 수 있는 가장 중요한 기술이다. 이는 망의 서비스 품질 제공 능력을 해당 망을 다른 망과 차별화시키는 데 가장 중요한 변수가 되며, 특히 전자상거래 등과 같은 미래의 통합 서비스 환경을 구축하는 데 가장 중요하다. 이는 단말기 또는 응용 서비스 특성에 맞게 망 자원을 최적으로 제어 해주기 때문에 가장 경제적인 망을 구축 및 운영할 수 있다.

마지막으로 광대역 통합망은 단순히 이종의 다양한 물리매체를 사용하는 기존의 유선망, 무선망 그리고 방송망을 통합하는 의미를 넘어서 사용자의 서비스 요구사항을 최적으로 만족시키면서, 망 자원을 가장 효과적으로 사용하게 하는 제어가 가능한 품질 보장망

을 구축하는 것이 매우 중요하다. 이러한 품질 보장망의 의미는 먼저 정보 전달을 통한 비즈니스를 지원하는 의미가 가장 크다고 할 수 있다. 이는 정보를 생성하고, 정보를 수집 및 처리하고, 정보를 전달하고, 그리고 정보를 이용하는 정보 먹이사슬 관계에서 안정되고 고품질의 통신망을 통하여 새로운 비즈니스를 창출할 수 있는 환경을 구축하는 것이다. 이는 네트워크가 단순히 정보를 공유하는 수단이 아니라 정보 자체의 가치를 매기는 수단이 되는 것이다. 이는 현재 인터넷이 단순히 접속 속도에 따라 요금을 부과하는 것이 아니고, 이용하는 정보의 형태와 사용 시간 그리고 정보 량에 따라 가치를 매길 수 있다. 그밖에 고품질 광대역통합망을 통하여 지금까지 응용 서비스 사업자나 개인으로 하여금 서로가 필요로 하는 정보 거래가 이루어질 수 있으며, 상호간에 많은 수익을 창출할 수 있다.

이러한 고품질 광대역통합망의 효과는 단순히 정보통신 산업뿐만 아니라 교통, 은행, 교육, 물류, 환경, 및 여행 등과 같은 타 산업의 생산성을 더욱 촉진시키는 의미가 있다. 따라서 고품질 광대역통합망은 9 대 신성장 산업을 비롯하여 우리나라 국민 소득을 2 만 달러 달성을 위한 가장 중요한 하부구조 역할을 담당할 것이다.

참 고 문 헌

공공기관 VoIPv6 참조모델 v2.0, 한국정보사회진흥원, 정보통신부

u-Korea 추진전략, 정보통신부, 2006

u-센서 네트워크 구축 기본 계획, 정보통신부

전국 경찰 전화망 고도화 방안 연구 보조 자료, 경찰청, 2007

리눅스 기반 사용자 모드 NAT-PT, IPv6 포럼코리아, 2001

전자통신동향분석 제21권 제5호, ETRI, 2006

김호성, "Security Issues on BcN", 2007 KrNET.

KISA, "광대역통합망(BcN) 주요장비에 대한 정보보호 가이드(V1.0), 2006. 12.

정교일, "BcN 인프라 보호를 위한 네트워크 보안기술의 발전 모델", 전자통신학회, 2004.03.10.

최재규, "RBAC을 이용한 ESM 모델연구" 주간기술동향 통권 1312호 2007.09.05

신명기, "IPv4/IPv6 연동 환경에서의 차세대 보안기술," 전자공학회지, 제33권 8호, 2006.

J-F. Mule, "SPEERMINT Requirements for SIP-based VoIP Interconnection," draft-ietf-speermint-requirements-01, October 23, 2006

UK Market", ENUM and VoIP Peering Forum, June, 2006.

Nordmark and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers," RFC 4213, Oct. 2005.

Business Communications Review

POLICE SCIENCE INSTITUTE