

# IPv6 표준화 동향 및 IPv4/IPv6 전환 기술

김형준 | TTA IPv6 전담반 의장  
ETRI 표준연구센터 차세대인터넷표준연구팀 팀장, 책임연구원

차세대 인터넷 주소체계인 IPv6는 BcN, 디지털홈, 유비쿼터스 컴퓨팅, GRID 등 21세기 국가경쟁력을 좌우하는 핵심인프라로 자리잡을 예정이다. 이번호에서는 우리나라가 IPv6 기반 차세대인터넷 상용화 구축과 기보유한 초고속/이동망 등, IPv6를 중심으로 한 유무선통합 및 망의 고도화를 앞당길 수 있도록 IPv6 특집을 구성하여 관련 기술동향을 살펴보고자 한다(편집자주).

## 1. IETF 표준화 동향

최근 북미, 유럽, 동북아를 중심으로 IPv6 도입 및 상용화에 대한 움직임이 매우 빠르게 전개되고 있어, 2005년을 기점으로 IPv6 시장 활성화에 일대 전환점을 맞이할 것으로 예상되고 있다. 지난 1994년, IETF의 IPng WG에서 IPv6 기본 규격이 표준화 된지 만 10년 만에 IPv6 상용화 움직임이 전 세계적으로 전개되고 있다. 이는 지난 1970년대, 현재의 IPv4 기반 인터넷 표준이 제정된 이후, 약 25년여의 시간이 흘러 오늘에 이르고 있는 경우에 비교하면 실로 IPv6의 보급 움직임은 그야말로 빠르게 진행되고 있는 셈이다. 오늘날, 기술이 곧 표준이고 표준이 곧 앞으로의 신규 시장을 선점할 수 있는 척도가 되는 글로벌 표준화 시대임을 감안하면 IPv6 기술 표준화 및 시험 인증에 대한 중요성은 더욱 강조될 전망이다.

IPv6 표준은 기존 32비트 주소 체계로 표현되는 IPv4 주소를 128비트 주소 체계로 확장하여 기존 인

### IPv6 특집 순서 ●●●●

#### ■ IPv6 표준화 동향 및 IPv4/IPv6 전환 기술

- Ad-hoc 네트워크에서의 IPv6 자동네트워킹 기술
- IPv6 이동성 지원 기술
- 국내 IPv6 응용 현황 및 전망
- IPv6 시험 기술
- IPv6 망구축 현황 및 보급전략

터넷이 안고 있는 근본적인 주소 고갈 문제를 해결하고, IPv6 기본 헤더를 단순화하여 패킷 처리의 성능 개선과 확장 헤더의 정의를 통한 이동성 지원, 보안 기능 제공, 서비스 품질 기능 등이 개선될 수 있도록 설계된 프로토콜이며, 특히 주소 자동설정 기능을 통한 플러그 앤 플레이 기능을 제공함으로써 손쉽게 이용자의 단말을 네트워크에 접속시킬 수 있도록 디자인되어 있다.

지난 1986년부터 활동을 시작한 IETF는 현재 100여 개의 WG이 8개의 Area로 나뉘어 인터넷 관련 표준을 만드는데 IPv6표준화는 IPng과 NGTrans WG을 중심으로 진행되어 왔다. 우선 IPng WG은 IPv6 기본 프로토콜 구조에 관한 규격을 제정해 온 그룹으로 IPv6 기본 규격과 IPv6 주소 자동 생성에 관한 표준을 제시하였다. NGTrans WG은 IPv4망에서 IPv6 적용 및 IPv6로의 전환을 위한 기존 망과의 상호 운용에 필요한 전환 메커니즘에 대한 표준화를 담당해 왔으며, 현재는 v6ops WG으로 명칭을 변경하여 IPv6

로의 전환 시나리오 작업과 IPv6 운용과 IPv6 응용 개발에 대한 가이드라인을 표준화 하고 있다. 이 밖에 IPv6 관련 IETF WG으로는 IP계층의 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.

우리나라의 IPv6 관련 국제 표준화 활동은 지난 1998년부터 선행적으로 추진되었으며 IETF에서의 본격적인 활동은 ETRI 표준연구센터를 중심으로 지난 2000년부터 시작되었다고 보여진다. 즉, 2000년대에 접어들면서 IETF 표준화 활동의 참석자 수 및 기고 활동이 점진적으로 증가하면서 IETF에서의 우리나라의 표준화 활동 노력이 인지되기 시작했으며, 지난 2002년 10월, 국내 최초로 IETF 국제 표준(RFC 3338, Bump In the API)이 채택되면서 IETF에서의 우리나라의 표준화 위상 제고에 커다란 전기가 마련되었다. 이후 지난 2003년 IETF에서의 우리나라의 기고서 제출 건 수 및 발표 건 수는 가파르게 상승하여 2002년도 대비 약 2배 이상의 상승 곡선을 이루기 시작했으며, 이러한 IETF 표준화 활동의 노력들이 모여 오는 59차 IETF 회의를 서울에서 유치하게 된 요인 중의 하나로 작용하지 않았나 생각된다.

이하 본 고에서는 우리나라의 IPv6 관련 주요 IETF WG별 이슈 현황을 간략히 정리하고, IPv4 기술 중 IPv4/IPv6 전환 기술에 대해 언급하고자 한다.

IPv6 WG(의장: Bob Hinden <hinden@iprg.nokia.com>, Brian Haberman <brian@innovationslab.net>)은 대부분의 작업이 완료되었으며, 금년 초 중에 표준화 활동을 마무리할 계획 하에 몇 가지 현안 위주의 논의 만이 진행되고 있다. 특히 지난 58차 미네아폴리스 회의에서는 site-local 주소를 대체하는 주소를 다루는 Bob Hinden의 “Unique

Local IPv6 Unicast Addresses” 문서의 WG Last Call에 대한 논의가 중점적으로 다루어졌으며, ETRI 표준연구센터에서 제안했던 “Link Scoped IPv6 Multicast Addresses”WG Draft에 대한 WG Last Call 절차가 진행되었으나, 본 WG Draft가 사용될 응용 분야를 수정 보완하여 차기 회의에서 재차 Last Call 절차를 거치는 것으로 협의된 바 있다. 따라서 오는 59차 서울 회의에서 본 WG Draft에 대한 최종 승인 절차 여부에 따라 우리나라는 두번째 RFC 표준 채택을 기대하고 있다.

v6ops WG(의장 : Robert Fink <bob@thefinks.com>, Pekka Savola <pekkas@netcore.fi>, Jonne Soininen <jonne.Soininen@nokia.com>)은 IPv6 전환을 위한 시나리오 작업 및 IPv6 운용과 IPv6 응용 개발에 대한 가이드라인을 표준화하는 WG이다. 현재 v6ops WG의 주요 표준화 이슈로는 3GPP, ISP, Enterprise, Unmanaged 망에서의 각각의 시나리오 및 솔루션에 대한 가이드라인 개발로, 현재 이를 위한 4개의 디자인 팀이 구성되어 작업 중에 있다. 현재 3GPP 시나리오 문서는 이미 RFC가 되었으며, Unmanaged 관련 문서들도 많은 작업이 진행된 반면, ISP 및 Enterprise 관련 문서들은 상대적으로 더디게 작업이 진행 중이다. 특히 지난 58차 IETF 회의에서는 새로운 WG 문서의 제안 발표로 Application Transition에 대한 논의가 있었으며, ETRI 표준연구센터에서 발표한 “draft-shin-v6ops-application-transition-02.txt” 기고서가 v6ops WG의 WG Draft로 채택되었다. 본 WG Draft는 금년 5월경 WG Last Call을 거쳐 빠르면 올해 안에 RFC 채택이 가능할 것으로 예상되며, 우리나라의 IETF 표준화 활동은 더욱 힘을 받을 수 있을 것으로 판단된다.

DNSOP(DNS Operations) WG(의장: David



Meyer <dmm@1-4-5.net>, Rob Austein <sra@hactrn.net>)에서는 DNS Deployment 및 Zone 파일 관리에 관련된 표준화 기술을 개발하고 있으며 지난 56차 회의에서부터 DNS Discovery에 대한 표준화가 진행되고 있다. DNS Discovery는 Stateful 및 Stateless 두 가지를 공히 지원하는 DHCPv6 기반의 DNS Discovery가 표준화 기술로 우세를 보이고 있지만, Stateless 방식의 RA(Router Advertisement) 기반 DNS Discovery 기술로, 현재 IPv6 RA 메시지에 빠져있는 Recursive DNS Server 주소를 알려주는 옵션을 포함할 것을 제안하며 주소자동설정과 같은 시나리오로 DHCPv6와 같이 사용되어야 한다는 논의도 함께 진행되고 있다. RA 기반 DNS Discovery는 계층적 MIPv6, 이동네트워크에서의 DNS 서버 주소를 알려주는데 적합할 뿐 아니라 이동통신에서 핸드폰을 통한 인터넷 서비스 시 IPv6 주소 자동설정과 DNS 서버 주소를 한번에 전달받을 수 있기 때문에 메시지 교환 측면에서 RA 기반의 DNS Discovery가 유리한 측면도 있다. 즉, 이동통신망에서는 대개 Stateless Address 주소 자동설정 기능을 통해 주소를 설정하기 때문에, DNS 정보도 함께 포함시켜 단말에게 알려주면 DHCPv6 서버 탐색 및 DNS 수신에 필요한 메시지 교환으로 인한 지연시간을 제거할 수 있는 장점이 있기 때문이다.

MIP(Mobile IP) WG은 최근에 들어 MIPv6의 기본 규격이 거의 마무리 단계에 와 있으나, RR(Return Routability) 등의 보안강화 작업 등의 일부 현안들을 남기고 있다. MIP 기본 규격은 망간 혹은 시스템간 로밍 서비스 제공에는 적합하나, 궁극적인 seamless mobility 제공을 위한 핸드오버(handover) 측면에서는 아직 개선해야 할 점이 많이 남아 있다. 즉, 세션을 유지하며 이동중인 단말에 대한 IP 핸드오버 기능을 제공하기에는 핸드오버 지연이 너무 커서 실시간 서비

스 제공에 부적합하며, 또한 바인딩 갱신 등의 제어 트래픽 오버헤드 및 확장성 문제는 여전히 미해결 문제로 남아 있다. 이러한 실시간 핸드오버 문제 및 제어 트래픽 오버헤드 문제를 다루기 위해, FMIPv6, HMIPv6 및 기타 MIPv6 최적화 이슈 등이 MIP WG에서 논의되고 있다.

## 2. IPv6 전환 기술 동향

IPv4/IPv6 전환 기술은 다음과 같이 크게 듀얼스택(Dual Stack), 터널링(Tunneling), 변환(Translation) 방식으로 구분된다.

### 2.1 듀얼 스택(Dual Stack)

듀얼 스택에 의한 IPv6로의 전환은 IPv4 기반의 기존 장비들이 IPv6도 지원하도록 업그레이드 하는 방식을 의미하며, 이는 추가적인 비용 부담이 적어 실제적인 IPv4 주소부족에 직면하기 전인 IPv6 도입 초기에 IPv4 기반 망 환경에서의 IPv6 지원 방안으로 선호될 것으로 보인다. 그러나 단말에서 IPv4 주소와 IPv6 주소 설정 모두를 요구하고, 라우터와 같은 네트워크 장비의 경우에는 IPv4 및 IPv6 라우팅 모두를 지원하여야 하기 때문에, 망 복잡도가 증가하고 망 관리 비용이 증가하는 문제를 안고 있다. 또한 기존 IPv4 주소의 부족 문제를 그대로 안고 있다.

### 2.2 터널링(Tunneling)

터널링은 전송하고자 하는 프로토콜의 정보가 다른 프로토콜 패킷 내에 캡슐화되어 전송되는 방식으로 크게 IPv4 기반 환경에서의 IPv6 터널링과 IPv6 기반

환경에서의 IPv4 터널링으로 분류할 수 있다.

IPv4 기반 IPv6 터널링은 IPv4 기반의 현 인터넷 환경하에서 IPv6 단말이나 IPv6 지역망들의 연결을 지원하기 위한 터널링 방안으로 IPv6 전환 초기와 중기까지 기존 망 환경에서의 점진적인 IPv6 전환을 위해서 널리 이용될 것으로 예상된다. 이러한 IPv4 기반 IPv6 터널링은 다시 설정 터널링 (Configured Tunneling)과 자동 터널링 (Automatic Tunneling) 방식으로 구분할 수 있다.

설정 터널링은 터널 종단 노드의 주소정보가 관리자에 의해서 설정되는 터널링 방식으로 6Bone이 대표적인 예가 된다. 이와 달리 자동 터널링에서는 수동설정 없이 IPv4-호환 (IPv4-compatible) 주소를 이용하여, IPv4 구간을 통과할 때 IPv4 호환 주소에 내포되어 있는 IPv4 주소를 터널 종단점 주소로 하여 자동으로 터널링 하게 된다. 최근에는 IPv4 호환 주소를 이용한 자동 터널링 보다 6to4나 ISATAP과 같은 향상된 자동 터널링 방식을 더 선호한다.

6to4는 하나 이상의 글로벌 IPv4 주소를 가지고 있는 IPv6 전용 사이트에 2001:⟨IPv4 주소⟩::/48 형태의 단일 IPv6 프리픽스를 할당하여 외부 IPv6 네트워크와의 자동 터널링을 지원한다. 이러한 6to4는 순수 IPv6를 지원하지 않는 광역 네트워크에 연결되어 있는 고립된 IPv6 사이트나 호스트가 자동 터널링 방식을 통해 다른 IPv6 도메인이나 호스트와 통신할 수 있도록 지원한다. 기본 메커니즘에 대한 표준화는 이미 완료되었으나 IETF의 v6ops WG을 통해 6to4에서의 보안 고려사항들에 대한 추가 Draft가 진행되고 있으며 6to4에서의 멀티캐스트 지원에 대한 논의도 미완료된 이슈로 남아있다.

설정 터널링이나 6to4가 IPv4 네트워크를 통한 IPv6 사이트간 연결을 지원하는데 이용되는 메커니즘이라면 IPv4 기반 환경에 있는 격리된 IPv6 호스트에

대한 IPv6 통신을 지원하는 터널링 기법으로는 6over4, ISATAP, 터널 브로커, TEREDO와 같은 메커니즘들이 있다.

6over4 메커니즘은 IPv4 사이트 내에서의 명시적인 터널 설정 없이 IPv6 호스트들 간의 연결을 지원하기 위해서 제안되었다. IPv4 주소를 인터페이스 식별자로 사용하며 IPv4 멀티캐스트를 IPv6 패킷 전송을 위한 가상링크로 이용한다. 그러나 IPv4 사이트 내에서의 IPv4 멀티캐스트 지원이 일반화되어 있지 않기 때문에 같은 기능을 지원하지만 이러한 제약이 없는 ISATAP 메커니즘이 더 선호될 것으로 예상된다.

ISATAP(Intra-Site Automatic Tunnel Addressing Protocol)은 고립된 IPv6/IPv4 듀얼 스택 호스트 사용자에게 IPv6 연결이 가능하도록 하는 자동 터널링 메커니즘으로 IPv6의 전개 과정 중 초기 모델에 적합한 방식이며 IPv4 망에서의 IPv6 듀얼 스택 노드의 점진적 도입 시에 적절한 메커니즘이라고 할 수 있다. ISATAP에서 사용되는 주소는 IPv6 임베디드된 IPv4주소(32bit)와 ISATAP 주소임을 알리는 프리픽스(Global prefix(64bit) + 0000:5EFE (32bit))와의 결합 형태를 사용하게 된다. IPv4 주소가 IPv6 주소에 임베디드 됨으로서 호스트와 외부 IPv6 연결성을 가지는 ISATAP 라우터 사이에 자동적인 IPv6 over IPv4 터널을 설정할 수 있다. ISATAP 호스트는 잘 알려진 DNS 이름이나 IPv4 애니캐스트를 통해 사이트의 ISATAP 라우터를 탐색할 수 있다. 또한 외부 연결성을 위해서 6to4와 결합되어 사용될 수도 있다.

터널 브로커(Tunnel Broker)는 IPv6 in IPv4 터널의 설정을 제공하는 웹 기반 톨로서 사용자가 웹 서버에 접속하면 우선 적절한 사용자 인증 및 허가 등의 사용자 접근제어를 거친 뒤 간단한 스크립트를 반환함으로써 이를 실행한 사용자 단말이 터널 브로커 서버로



IPv6 in IPv4 터널을 자동 설정하게 한다. 이처럼 터널 브로커는 글로벌 IPv4 주소를 가졌지만 IPv6 망에 대한 직접적인 접속을 가지지 못한 듀얼 스택 노드에 간단한 방식으로 IPv6 접속을 제공받을 수 있게 한다. 이를 이용한 대표적인 서비스의 예로 freenet6 가 있다.

Teredo는 IPv4 네트워크의 NAT 도메인에 존재하는 듀얼스택 호스트의 IPv6 네트워크로의 원활한 통신을 지원하기 위한 메커니즘이다. NAT는 cone NAT, restricted NAT, symmetric NAT로 구분되며, Cone NAT는 내부 주소와 포트에 대해 매핑되어지는 주소 및 포트에 매핑 테이블이 구성되고, restricted NAT는 cone NAT의 매핑 테이블에 목적지 주소가 포함된다. symmetric NAT는 cone NAT의 매핑 테이블에 목적지의 주소 및 포트가 포함된다.

Teredo 메커니즘은 Teredo 클라이언트, Teredo 서버, Teredo 릴레이 시스템으로 구성된다. Teredo 클라이언트는 IPv4 NAT 도메인에 존재하는 듀얼스택 호스트에 위치하며 Teredo 서버의 주소를 받아 IPv6 주소를 생성한다. 단말에서 생성된 IPv6 패킷은 UDP와 IPv4로 캡슐화된다. IPv4 헤더의 주소에 Teredo 클라이언트의 IPv4 주소가 저장된 후에, NAT의 의해 NAT mapped 주소로 변환되어 Teredo 릴레이 시스템으로 전달된다. Teredo 릴레이 시스템은 IPv4 헤더와 UDP 헤더를 제거한 후 IPv6 네트워크로 릴레이하여 패킷을 IPv6 목적지까지 전달한다. Cone NAT에서는 이러한 메커니즘이 적용되지만 restricted NAT인 경우에는 목적지 주소를 매핑 테이블에 가지고 있기 때문에 Teredo 클라이언트의 연결 요청이 선행되지 않고 IPv6 호스트가 먼저 Teredo 클라이언트에 연결 요청을 하면 NAT에서 해당 패킷이 폐기된다. 따라서 이 경우 버블 패킷과 origin indicator를 사용하여 필요한 매핑 목록을 매핑 테이블

에 저장하는 복잡한 추가 과정이 필요하다. 또한 symmetric NAT의 경우에는 Teredo 메커니즘이 지원되지 않는다. 이처럼 Teredo는 그 구성이 복잡하고 적용되는 환경에서의 NAT의 유형에 따라 동작이 지원되지 않을 수도 있어 IPv6를 지원하지 않는 NAT 환경에서만 제한적으로 쓰일 것으로 예상된다.

IPv6 도입이 진행될수록 IPv6 기반 망이 확대되어 IPv6 기반 IPv4 터널링의 이용이 확대될 것이다. IPv6 기반 망을 통한 고립된 IPv4 사이트의 연결을 지원하기 위해서는 IPv4 in IPv6 터널링 형태의 설정 터널링이 사용될 수 있다. 또한 IPv6 기반 망에서의 고립된 IPv4 단말에 대한 IPv4 통신을 지원하기 위해 DSTM 메커니즘이 사용될 수 있다.

DSTM은 IPv6기반 망에서 IPv4/IPv6듀얼 스택을 탑재한 단말이, IPv4 통신 요구 시에 DSTM 서버로부터 동적으로 IPv4 주소를 할당 받아, IPv4 in IPv6 터널링을 통하여 IPv4/IPv6 경계 라우터(DSTM TEP)로 패킷을 전달하고, DSTM TEP에서 IPv4 패킷으로 복원하여 IPv4 망으로 전달 함으로서, IPv4 망과의 투명한 연동을 제공하는 메커니즘이다. DSTM에 의한 IPv4 in IPv6 터널링은 IPv6 기반 망 내의 단말에서 IPv4 응용들을 그대로 사용할 수 있게 한다. 또한 동적인 IPv4 주소 할당 메커니즘은 IPv4 주소 활용도를 제고한다. DSTM의 이러한 특성은 신규 도입 망이 IPv6 기반 망으로 구축되도록 기여할 수 있을 것으로 기대된다. 또한 IPv6 기반 망 도입이 확대되는 IPv6 도입 중반 이후로 갈수록 그 필요성이 증가될 것으로 예상된다.

### 2.3 변환 메커니즘(Translation)

터널링 메커니즘으로는 듀얼 스택을 지원하지 않는 IPv6 전용 단말과 IPv4 단말사이의 통신을 지원할 수

없다. 이러한 이기종 프로토콜간 통신을 지원하기 위해서는 변환(Translation)에 기반한 메커니즘이 필요하다. 이러한 변환 메커니즘은 변환이 수행되는 계층에 따라 헤더 변환 방식, 전송계층 릴레이 방식, 응용계층 게이트웨이 방식으로 분류할 수 있다. 헤더 변환 방식의 메커니즘으로는 SIIT, NAT-PT가 있다. 헤더 변환은 IP 계층에서의 변환으로 IPv6 패킷 헤더와 IPv4 헤더 사이의 변환과 그에 따르는 체크섬의 조정을 가리킨다. 또한 ICMPv6와 ICMPv4 사이의 변환도 요구되며 이러한 변환 규칙을 SIIT에서 정의하고 있다.

NAT-PT는 SIIT에 기반을 둔 헤더 변환 방식의 전형적인 예이다. NAT-PT는 SIIT의 프로토콜 변환알고리즘 뿐 아니라 기존의 NAT의 동적주소 변환 기술과, 응용 프로토콜 변환 기술들을 통합한 메커니즘으로 종단 단말들의 수정 없이 IPv6 호스트와 IPv4 호스트 사이의 통신을 지원한다. 이러한 변환 방식은 NAT에서와 같이 IP 계층 변환에 따른 제약점들을 가지고 있다. 대표적인 제약점으로 DNS, FTP와 같이 응용 프로토콜에 내장된 IP 주소 변환의 어려움을 들 수 있으며 이를 지원하기 위해서 DNS ALG, FTP ALG와 같은 별도의 응용 게이트웨이가 추가로 구현되어야 한다. 이것은 응용이 교환하는 데이터에 IP 주소가 내장되는 경우, 이에 대한 변환을 지원하기 위한 추가적인 ALG가 구현되어야 함을 의미하며 추가적인 서비스 도입을 어렵게 하는 요인이 된다. 또한 ICMPv4와 ICMPv6사이의 차이로 인하여 변환에 따른 정보 손실이 발생할 수도 있다. 또한 패킷 변환의 특성상 IPSec과 같은 보안프로토콜에 의한 종단간 보안을 지원할 수 없다는 단점도 있으나 최근 NAT를 통한 IPSec 지원 방안이 제안되어 제한적인 IPSec의 지원이 가능하다. 이러한 여러가지 제약점에도 불구하고 헤더변환 방식은 종단 단말의 변경을 요구하지 않는다

는 장점과 듀얼스택이 지원되지 않는 IPv6 전용 장치들에 대한 IPv4 연동을 지원할 있다는 점들로 인해서 해당분야의 연동 기술로 활용될 것이다. 최근 NAT-PT의 Applicability에 대한 고려의 필요성이 제기되어 추가적인 이슈로 논의될 것으로 보여진다.

Bump in the Stack(BIS)는 SIIT와 연계된 NAT-PT 방식과 유사하며 각 단말의 프로토콜 스택상에 구현되어 IPv4 응용에 의하여 생성되는 IPv4 트래픽을 IPv6 트래픽으로 변환하여 IPv6 망으로 전달하며 또한 그 역과정도 수행한다. 따라서 NAT-PT와 같이 응용이 IPv6 주소를 내포하고 있을 경우 그에 대한 추가적인 ALG 지원이 요구된다.

Bump in the API(BIA)는 단말상에서 적용되어 IPv4 응용에 의한 IPv6 응용과의 통신을 지원한다는 점에서 BIS와 유사하지만 소켓 API 레벨에서 IPv4 소켓에 대한 IPv6 소켓으로의 변환 및 그 역과정을 수행한다는 점에서 차이를 가진다. 소켓 API 레벨의 변환이기 때문에 패킷 헤더 변환이나 IPv4 주소를 내제하는 응용을 지원하기 위한 추가적인 ALG가 요구되지 않아 IPv6 응용으로의 전환이 불가한 IPv4 응용들을 IPv6 단말에서 사용하기 위한 방안으로 사용될 수 있다.

전송계층 릴레이 방식은 {TCP,UDP}/IPv4 세션과 {TCP,UDP}/IPv6 세션을 중간에서 릴레이 하는 방식으로 TRT, SOCKS 게이트웨이 방식이 이에 해당된다. 이러한 방식은 IPv6 전용 단말이 IPv4 전용 단말과 UDP나 TCP에 의한 통신을 가능하게 한다. 이러한 방식은 그 변환이 전송계층에서 이루어짐으로 IP 계층의 헤더변환이나 ICMP 변환은 요구되지 않는다. 그러나 응용 프로토콜에 내장된 IP 주소의 변환과 같은 문제는 여전히 남아 있다.

응용계층 게이트웨이(ALG) 방식의 경우, 응용 클라이언트는 트랜잭션 요구를 응용서버가 아닌 ALG에게



보내고 ALG가 그러한 요구를 클라이언트를 대신하여 응용서버에 전달하고 서버로부터의 응답을 클라이언트에게 릴레이 한다. 이러한 ALG의 전형적인 예로 웹 캐쉬나 프락시를 들 수 있다. SMTP 서버또한 ALG의 형태로 보여질 수 있다.

## 2.4 IPv6 전환기술의 향후 과제

IPv6 전환기술 개발 및 표준화를 담당했던 ngtrans WG이 종료되면서 ISATAP, TEREADO, DSTM과 같은 표준화가 완료되지 못한 IPv6 전환메커니즘들은 Experimental RFC로의 개별표준화를 진행하도록 권고되었고, 현재 개별 Draft로 제출된 상

태이나 ngtrans WG의 역할을 넘겨받은 v6ops WG에 의한 IPv6 도입 시나리오 작업이 완료되어야 표준화 여부가 결정될 것으로 보인다. 이와 별도로 이들 메커니즘들은 산업계의 각 장비에 의한 지원 및 사용이 진행되고 있어 산업계의 Defacto 표준으로 먼저 자리잡을 것으로 예상된다. IETF에 의해 다양한 IPv6 전환기술이 개발되고 표준화 되었지만 각 전환 메커니즘 간의 상호 활용성, 각 메커니즘에서의 보안 및 멀티캐스트에 대한 고려, 각 변환 및 터널링 기법들의 네트워크 성능에 미치는 영향 등에 대한 다각적인 연구가 아직 미진한 상태이며, 따라서 이러한 연구에 대한 앞으로의 관심과 지원이 요구된다. **TTA**

