IPv6 전환기술 동향 및 과제

이 희 천*　　김 형 준**

◈ 목 차 ◈

1. 서 론

IPv4 (Internet Protocol version 4)에 기반한 현재의 인터넷은 사용자의 급속한 증가로 인해 주소고갈 문제에 직면하고 있으며, 새롭게 등장하고 있는 휴대 인터넷, 홈네트워크 등의 신규 서비스들은 인터넷 주소 고갈을 더욱 앞당길 것으로 예상된다. 이러한 주소 부족 문제를 해결하기위해서 IETF는 IPv6 (Internet Protocol version 6)를 개발하였고 IPv6 이제 그 표준화가 완료되어 도입기에 들어서고 있다.

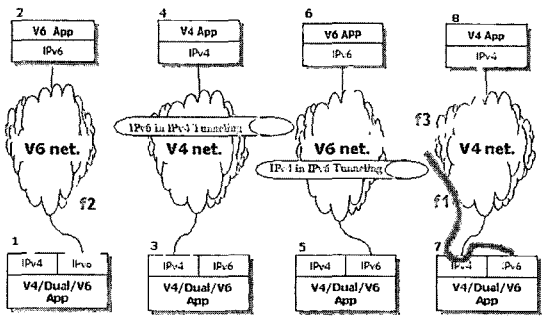
IPv6는 128 비트 주소 체계를 제공하여 거의 무한한 주소공간을 제공할 수 있다. 또한 단순화된 헤더, 주소 자동설정, 효율적인 이동성 지원 등 다양한 장점들로 인하여 기존 인터넷의 기반이되는 인터넷 프로토콜인 IPv4를 대체할 차세대 인터넷 프로토콜로 인정받고 있다[1]. 또한 IPv6는 인터넷의 영역을 사물들에까지 확대하는 차세대 통신패러다임으로 대두되고 있는 유비쿼터스 네트워크를 실현 시킬 기반 기술로서도 그 중요성을 가진다. 그러나 IPv6는 IPv4와 호환되지 않고 또한 이미 전세계를 아우르는 거대한 인터넷이 IPv4에 기반하여 운영되고 있어 점진적인 IPv6로의 전환이 불가피하다. 이는 상당 기간 동안 IPv4 망과 IPv6 망이 공존하게 됨을 의미한다. 따라서 IPv6 망과 IPv4 망사이의 투명한 연동을 지원하는 IPv6 전환기술의 개발 및 지원이 주요한 이슈로 대두되었고 IETF의 Ngtrans WG을 중심으로 다양한 연동기술이 개발되었다. Ngtrans WG을 이어받은 v6ops WG에서는 개발된 연동 기술을 기반으로 각 네트워크 영역에서의 IPv6 도입 시나리오의 개발을 진행하고 있다.

그림 1은 IPv4 망과 IPv6 망이 공존하는 네트워크 환경에서 발생할 수 있는 다양한 통신 유형들과 그에 따라 요구되는 IPv6 전환 기술들의 유형을 보여준다.

본 고에서는 IPv6 망과 IPv4 망이 공존하는 네트워크 환경에서 투명한 IPv4 와 IPv6 사이의 연동을 지원하기 위해서 개발된 다양한 IPv6 전환 기술들을 고찰하고 IPv6 전환 기술 분야에서 추가적인 고려사항들을 살펴본다.

2. IPv6 전환 기술 동향

IPv6 전환 기술을 크게 듀얼 스택, 터널링(Tunneling), 변환(Translation) 방식으로 구분할 수 있다.



(그림 1) IPv6와 IPv4 가 공존하는 네트워크 모델

* 한국전자통신연구원 선임연구원
** 한국전자통신연구원 차세대인터넷표준연구팀 팀장

2.1 듀얼 스택 (Dual Stack)

듀얼 스택에 의한 IPv6로의 전환은 IPv4 기반으로 구축된 호스트나 라우터와 같은 네트워크 장비들이 IPv4와 IPv6 통신을 모두 지원하도록 업그레이드 하는 방식으로 기존 장비에서의 IPv6 지원을 위한 업그레이드는 추가적인 비용 부담이 적어 실제적인 IPv4 주소부족에 직면하기전인 IPv6 도입 초기에는 IPv4 기반 망 환경에서의 IPv6 지원 방안으로 선호될 것으로 보인다. 그러나 이를 지원하는 단말은 IPv4 주소와 IPv6 주소 설정 모두를 요구하고, 라우터와 같은 네트워크 장비의 경우에는 IPv4 및 IPv6 라우팅 모두를 지원하여야 하기 때문에, 망 복잡도가 증가하고 망관리 비용이 증가하는 문제를 안고 있다. 또한 기존 IPv4 주소부족 문제를 그대로 안고 있다.

2.2 터널링 메커니즘 (Tunneling)

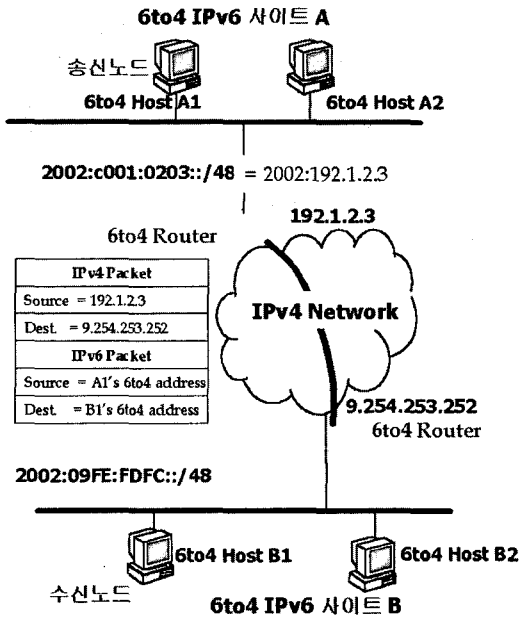
터널링은 전송하고자 하는 프로토콜의 정보가 다른 프로토콜 패킷내에 캡슐화 되어 전송되는 방식으로 크게 IPv4 기반 환경에서의 IPv6 터널링과 IPv6 기반 환경에서의 IPv4 터널링으로 분류할 수 있다.

2.2.1 IPv4 기반 IPv6 터널링

IPv4 기반 IPv6 터널링은 IPv4 기반의 현재의 인터넷과 망 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[2].

설정 터널링은 터널 종단 노드의 주소정보가 관리자에의해서 설정되는 터널링방식으로 그림 1의 IPv6 in IPv4 Tunneling이 이에 해당하며 이를 이용하여 구축된 국제적인 IPv6 시험 망으로 6Bone을 들 수 있다.

자동 터널링에서는 IPv4-호환 (IPv4-compatible) 주소를 이용하여 매뉴얼한 설정 없이, IPv4 구간을 통과할 때 IPv4 호환 주소에 내포되어 있는 IPv4 주소를 IPv4 터널 종단점 주소로 하여 자동으로 터널링하게 된다.



(그림 2) 6to4를 이용한 고립된 IPv6 망간의 연결

최근에는 IPv4 호환 주소를 이용한 자동 터널링보다 6to4나 ISATAP과 같은 향상된 자동 터널링 방식을 더 선호한다.

6to4[3]는 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. 그림 2는 6to4에 의하여 고립된 IPv6 사이트가 연동하는 시나리오를 보여주고 있다. 이처럼 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.

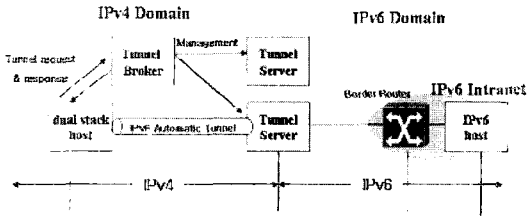
최근 IETF의 v6ops WG을 통해 6to4에서의 보안고려사항들에 대한 추가 드래프트가 진행되고 있으며 6to4에서의 멀티캐스트 지원에 대한 논의도 미완료된 이슈로 남아있다[4].

설정 터널링이나 6to4가 IPv4 네트워크를 통한 IPv6 사이트간 연결을 지원하는데 이용되는 메커니즘이라면 그림 1의 f1과 같이 IPv4 기반 환경에 있는 IPv6 호스트의 IPv6 통신을 지원하는 터널링 기법으로는 6over4, ISATAP, 터널 브로커, TEREDO와 같은 메커니즘들이 있다.

6over4[5] 메커니즘은 IPv4 사이트 내에서의 명시적인 터널 설정없이 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) [6]은 고립된 IPv6/IPv4 듀얼 스택 호스트 사용자에게 IPv6 연결 가능하도록 하는 자동 터널링 전환 메커니즘이다. IPv6의 전개 과정 중 초기 모델에 적합한 방식으로서 순수한 IPv4 망에서 IPv6 듀얼스택 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. 이와 같이 IPv4 주소가 IPv6 주소에 임베디드되므로 호스트와 외부 IPv6 연결성을 가지는 ISATAP 라우터 사이에 자동적으로 IPv6 over IPv4 터널을 설정할 수 있다. ISATAP 호스트는 Well-known DNS 이름이나 IPv4 에니캐스트를 통해 사이트의 ISATAP 라우터를 탐색할 수 있다. 이러한 ISATAP 메커니즘은 외부 연결성을 위해서 6to4와 결합되어 사용될 수도 있다.

터널 브로커 (Tunnel Broker) [7]는 IPv6 in IPv4 터널의 설정을 제공하는 웹기반 툴로서 사용자가 웹서버에 접속하면 우선 적절한 사용자 인증 및 허가 등의 사용자 접근제어를 거친뒤 간단한 스크립트를 반환함으로서 이를 실행한 사용자 단말이 터널 브로커 서버로 IPv6 in IPv4 터널을 자동 설정하게 한다. 그림 3은 이러한 과정을 보여주고 있다.



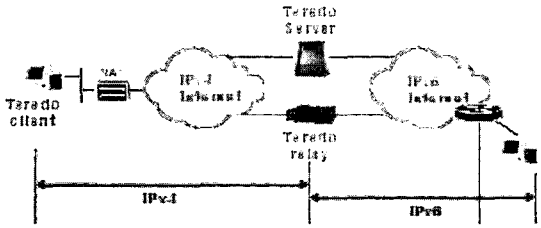
(그림 3) Tunnel Broker를 통한 IPv6 망 접속

이러한 터널 브로커 방식은 사용가능한 글로벌 IPv4 주소를 가진 듀얼 스택 노드에게 간단한 방식으로 IPv6 네트워크 접속을 지원할 수 있게 함으로서 IPv6 망에 대한 직접적인 접속을 가지지 못한 IPv4 사용자들이 손쉽게 IPv6 접속을 제공받을 수 있는 방안이다. 이를 이용한 대표적인 서비스의 예로 freenet6 가 있다[8].

Teredo[9]는 IPv4 네트워크의 NAT 도메인에 존재하는 듀얼스택 호스트와 IPv6 네트워크의 IPv6 호스트사이의 원활한 통신을 지원하기 위한 메커니즘이다. NAT는 cone NAT, restricted NAT, symmetric NAT로 구분된다. Cone NAT는 내부 주소와 포트에 대해 매핑되어지는 주소 및 포트로 매핑 테이블이 구성 되고, restricted NAT는 cone NAT의 매핑 테이블에 목적지 주소가 포함된다. symmetric NAT는 cone NAT의 매핑 테이블에 목적지의 주소 및 포트가 포함된다.

Teredo 메커니즘의 구성요소들은 Teredo 클라이언트, Teredo 서버, Teredo 릴레이 시스템으로 구성된다. Teredo 클라이언트는 IPv4 NAT 도메인에 존재하는 듀얼스택 호스트로 Teredo 서버의 주소를 받아 IPv6 주소를 생성한다. Teredo 메커니즘은 기본적으로 IPv6 패킷을 생성한 후, UDP와 IPv4 IP로 캡슐화된다. IPv4 IP 헤더의 주소는 Teredo 클라이언트의 IPv4 주소로 저장된 후에, NAT의 의해 NAT mapped 주소로 변환되어 Teredo 릴레이 시스템으로 전달된다. Teredo 릴레이 시스템은 IPv4 헤더와 UDP 헤더를 제거한 후 IPv6 네트워크로 릴레이하여 IPv6 목적지까지 전달된다.

Cone NAT에서는 이러한 기본적인 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 버려진다. 따라서 restricted NAT의 경우



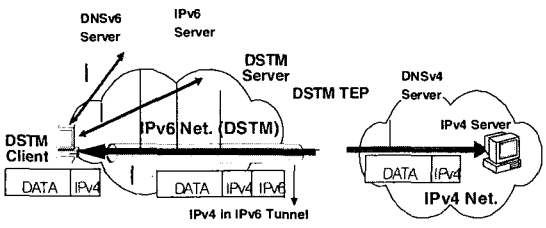
(그림 4) Teredo를 통한 IPv6 망 접속

bubble packet과 origin indicator를 사용하여 필요한 매핑 목록을 매핑 테이블에 저장하는 복잡한 추가 과정이 필요하다. 또한 symmetric NAT의 경우에는 Teredo 메커니즘이 지원되지 않는다. 이처럼 Teredo는 그 구성이 복잡하고 적용되는 환경에서의 NAT 의 유형에 따라 동작이 지원되지 않을 수도 있어 IPv6를 지원하지 않는 NAT 환경에서만 제한적으로 쓰일 것으로 예상된다.

2.2.2 IPv6 기반 IPv4 터널링

IPv6 도입이 진행될수록 IPv6 기반망이 확대되어 IPv6 기반 IPv4 터널링의 이용이 확대될 것이다. IPv6 기반망을 통한 고립된 IPv4 사이트의 연결을 지원하기 위해서는 그림1의 IPv4 in IPv6 Tunneling과 같은 형태의 설정터널링이 사용될 수 있다. 그림 1의 f2와 같이 IPv6 기반망에서 단말이 IPv4 통신을 통해 IPv4 망으로 접속하는 것을 지원하는 IPv6 기반 IPv4 터널링 기법으로 DSTM (Dual Stack Transition Mechanism)이 제안되었다 [10].

DSTM은 IPv6기반 망에서 IPv4/IPv6듀얼스택을 탑재한 DSTM단말이, IPv4 통신 요구시에 DSTM 서버로부터 동적으로 IPv4 주소를 할당 받아, IPv4 in IPv6 터널링을 통하여 IPv4/IPv6 경계라우터(DSTM TEP)로 패킷을 전달하고, DSTM TEP에서 IPv4 패킷으로 복원하여 IPv4 망으로 전달함으로서, IPv4 망과의 투명한 연동을 제공한다. 그림 5는 DSTM에 의한 IPv6 기반 망내의 단말에 대한 IPv4 통신의 과정을 보여주고 있다. 이처럼 DSTM은 IPv6 기반 망을 구성하면서도 IPv4 in IPv6 터널링에 의한 투명한 IPv4 망과의 연동을 제공할 수 있고, IPv6망내의 단말에서 IPv4기반 응용들을 그대로 사용할 수 있게 한다. 또한 동적인 IPv4 주소 할당 메커니즘을 제공하여 IPv4 주소 활용도를 제고한다. DSTM의 이러한 특성은 IPv6 기반 망으로 구축하더라도 IPv4 망과의 투명한 연동을 보장함으로서 신규도입 망 영역에서의 IPv6 기반망 구축의 촉진에 기여할 것으로 기대된다. 또한 IPv6 기반망 도입이 확대되는 IPv6 도입 중반 이후로 갈수록 그 필요성이 증가될 것으로 예상된다.



(그림 5) DSTM에 의한 IPv6/IPv4 연동

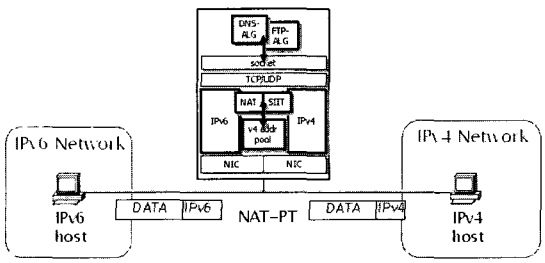
2.3 변환 메커니즘 (Translation)

터널링 방식의 IPv6 전환 메커니즘으로는 듀얼스택을 지원하지 않는 IPv6 전용 단말과 IPv4 단말사이의 통신을 지원할 수 없다. 이러한 이기종 프로토콜간 통신을 지원하기 위해서는 그림 1의 f3과 같은 변환(Translation) 방식에 기반한 메커니즘이 필요하다. 이러한 변환 방식의 메커니즘은 변환이 수행되는 계층에따라 헤더 변환 방식, 전송계층 릴레이 방식, 응용계층 게이트웨이 방식으로 분류할 수 있다.

헤더 변환 방식의 변환메커니즘으로는 SIIT, NAT-PT가 있다[11][12]. 헤더 변환은 IP 계층에서의 변환으로 IPv6 패킷 헤더와 IPv4 헤더사이의 변환과 그에 따르는 체크섬의 조정을 가리킨다. 또한 ICMPv6와 ICMPv4 사이의 변환도 요구되며 이러한 변환 규칙을 SIIT 에서 정의하고 있다.

NAT-PT는 이러한 SIIT에 기반을 둔 헤더 변환 방식의 전형적인 예이다. NAT-PT는 SIIT의 프로토콜 변환 알고리즘 뿐아니라 기존의 NAT의 동적주소 변환 기술과, 응용 프로토콜 변환 기술들을 통합한 메커니즘으로 종단 단말들의 수정없이 IPv6 호스트와 IPv4 호스트 사이의 통신을 지원할 수 있다.

그림 6은 이러한 NAT-PT를 통한 IPv6와 IPv4 망간 연동을 보여주고 있다. 그러나 이러한 변환 방식은



(그림 6) NAT-PT에 의한 IPv4/IPv6 연동

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 지원하기위해서 각각 그에 맞는 추가적인 ALG가 구현되어야 함을 의미함하며 이는 추가적인 서비스 도입을 어렵게 하는 요인이 될 수 있다. 또한 ICMPv4와 ICMPv6사이의 차이로 인해서 정확한 변경이 불가한 부분도 있어 변환으로 인한 정보의 손실이 발생할 수도 있다. 또한 패킷변환의 특성상 IPSec과 같은 보안프로토콜에 의한 종단간 보안을 지원할 수 없다는 단점도 있으나 최근 NAT를 통한 IPSec 지원 방안이 제안되어 제한적인 IPSec의 지원이 가능하다[13]. 이러한 여러가지 제약점에도 불구하고 헤더변환 방식은 종단 단말의 변경의 요구하지 않는다는 장점과 듀얼스택이 지원되지 않는 IPv6 전용 장비들에 대한 IPv4 연동을 지원할 있다는 점들로 인해서 해당분야의 연동 기술로 활용될 것이다. 최근 NAT-PT의 Applicability에 대한 고려의 필요성이 제기되어 NAT-PT에 대한 추가적인 이슈로 논의될 것으로 보여진다.

Bump in the Stack(BIS) [14]는 SIIT와 연계된 NAT-PT 방식과 유사하며 각 단말 운영체제의 프로토콜 스택상에 구현되어 IPv4 응용의해 생성되는 IPv4 트래픽을 IPv6 트래픽으로 변환하여 IPv6 망으로 전달하며 또한 그 역과정도 수행한다. 따라서 NAT-PT와 같이 응용이 IPv6 주소를 내포하고 있을경우 그에 대한 추가적인 ALG 지원이 요구된다.

Bump in the API (BIA) [15]는 단말상에서 적용되어 IPv4 응용에 의한 IPv6 응용과의 통신을 지원한다는 점에서 BIS와 유사하지만 듀얼스택 단말의 소켓 API 레벨에서 IPv4 소켓에 대한 IPv6 소켓으로의 변환 및 그 역과정을 수행한다는 점에서 차이를 가진다. 그 변환이 소켓 API 레벨에서 이루어지기 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 방식는 {TCP,UDP}/IPv4 세션과 {TCP,UDP}/IPv6 세션을 중간에서 릴레이 하는 방식으로 TRT[16], SOCKS[17] 게이트웨이 방식이 이에 해당된다. 이러한 방식은 IPv6 전용 단말이 IPv4 전용 단말과 UDP나 TCP에의한 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 릴레이한다. 이러한 ALG의 전형적인 예로 웹 캐쉬나 프락시를 들 수 있다. SMTP 서버또한 ALG의 형태로 보여질 수 있다.

3. IPv6 전환기술의 향후 과제

IPv6 전환 기술 개발 및 표준화를 담당했던ngtrans WG이 종료되면서 ISATAP, TEREDO, DSTM과 같은 표준화가 완료되지 못한 IPv6 전환메커니즘들은 Experimental RFC로의 개별표준화를 진행하도록 권고 되었다. 현재 각각 새롭게 수정되어 개별 드래프트로 제출된 상태이나 ngtrans WG의 역할을 넘겨받은 v6ops WG에의한 IPv6 도입 시나리오 작업이 완료되어야 표준화여부가 결정될 것으로 보인다. 이와 별도록 산업계의 각 장비에 의한 지원 및 사용이 진행되고 있어 이들 메커니즘들은 산업계의 Defacto 표준으로 먼저 자리잡을 것으로 보인다. 또한 v6ops WG에 의한 시나리오 개발에서 각 영역의 연동 메커니즘으로 포함될지의 여부에 따라 해당 메커니즘의 향후 표준화 진행의 향방도 결정될 것이다.

v6ops WG에서는 Unmanaged, Enterprise, ISP, 3GPP 네트워크 분야로 크게 나누어 각각의 네트워크가 안정적이고 빠른 IPv6로의 전환을 위한 특징들과 기본 시나리오 및 요구사항을 개발하고 있다. 그 중에 적용영역이 가장 명확한 3GPP에서의 적용시나리오의 개발 및 표준화가 가장 빠르게 진행되어 기본 시나리오에 대한 표준화를 마무리하였다[18]. 또한 Unmanaged

[19]와 ISP[20], Enterprise[21]에서의 적용시나리오 작업이 그 뒤를 따르고 있어 차년도인 2004년도에는 4개 영역에서의 적용 시나리오 개발 작업이 마무리 될 것으로 예상된다.

많은 IPv6 전환기술이 개발되고 IETF에 의해 표준화되었지만 각 전환메커니즘간의 상호활용성, 각 메커니즘에서의 보안 및 멀티캐스트에 대한 고려, 각 변환 및 터널링 기법들의 네트워크 성능에 미치는 영향 등에 대한 다각적인 연구가 아직 미진한 상태이다. 따라서 이러한 부문에 대한 부가적인 연구가 요구된다. 이미 구축된 거대한 IPv4 기반 망에서의 IPv6 지원방안에 대한 연구도 중요하지만, 향후 등장할 새로운 신규 망 및 서비스들을 IPv6 기반 환경으로 유도하는 노력도 간과되어서는 안된다. 신규 서비스 및 망들이 IPv4 기반 망으로 구축될 경우 차 후에 또 다시 IPv6 기반 망으로 전환하는 추가 비용이 발생할 수 밖에 없다. 따라서 홈네트워크 및 휴대 인터넷 등 새롭게 고려되고 있는 신규 망 및 서비스는 IPv6 기반 환경에서 IPv4 연동을 지원하는 방향으로 그 도입이 검토되어야 할 것이다. 또한 이와 함께 IPv6 기반 통신 환경을 지원하는 운영체제의 지원도 뒤따라야 할 것이다.

4. 결 론

본 고에서는 IETF에 의해서 개발된 IPv6 전환기술을 IPv4 기반 IPv6 터널링, IPv6 기반 IPv4터널링, 변환 메커니즘으로 분류하여 살펴보았다. 이미 6to4, NAT-PT등 대부분의 IPv6전환 메커니즘은 그 개발 및 표준화가 완료되었고 Applicability 및 보안 고려사항 등이 추가적인 이슈로 고려되고 있다. 그러나 ISATAP, TEREDO, DSTM은 표준화가 마무리되지 않고 ngtrans WG이 종료됨에 따라 Experimental RFC로의 개별표준화가 진행중이다. 또한 이러한 메커니즘들의 표준화는 v6ops WG에 의한 시나리오 작업이 마무리되어야 그 진행의 여부가 결정될 것으로 보여, 각 장비에 의한 지원 및 사용이 선행되어 산업계 Defacto 표준으로 먼저 자리잡을 것으로 보인다.

많은 IPv6 전환기술들이 개발되었다. 그러나 각기술들은 그 적용성이 달라 각 기술간 연계의 필요성 및 상호작용에 대한 고려가 필요하다. 또한 변환 및 터널링 기법들의 네트워크 성능에 미치는 영향 등과 같은 각 전환기술들에 대한 평가도 IPv6 전환의 가이드라인을 제공하는 척도로서 추가적인 연구가 요구된다. 또한 기존 IPv4 망에대한 IPv6의 지원뿐 아니라 새로이 등장하고 있는 신규 서비스들의 IPv6 기반 환경으로의 도입 노력도 간과되어서는 안된다. 또한 이를 지원하기 위해서는 운영체제의 IPv6 기반 환경 지원이 요구된다.

참고문헌

[1] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, December 1998.

[2] R. Gilligan, E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers," RFC 2893, August 2000.

[3] B. Carpenter, K. Moore, "Connection of IPv6 Domains via IPv4 Clouds," RFC 3056, February 2001.

[4] P. Savola, "Security Considerations for 6to4," Internet Draft, <draft-ietf-v6ops-security-00.txt>, October 2003.

[5] B. Carpenter and C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels," RFC 2529, March 1999.

[6] F. Templin, T. Gleeson, M. Talwar, D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)," Internet Draft, <draft-ietf-ngtrans-isatap-16.txt>, October 2003.

[7] A. Durand, P. Fasano, I. Guardini, and D. Lento, "IPv6 Tunnel Broker," RFC 3053, June 2001.

[8] The Freenet6 Tunnel Broker, http://www.freenet6.net/

[9] C. Huitema, "Teredo: Tunneling IPv6 over UDP through NATs," Internet Draft, <draft-huitema-v6ops-teredo-00.txt>, June 2003.

[10] J. Bound, L. Toutain, O. Medina, F. Dupont, M. Shin, J. Lee, H. Lee, E. Castro, "Dual Stack Transition Mechanism" Internet Draft, <draft-bound-dstm-exp-00.txt>, August 2003.

[11] E. Nordmark, "Stateless IP/ICMP Translation Algorithm (SIIT)," RFC 2765, February 2000.

[12] G. Tsirtsis, and P. Srisuresh, "Network Address Translation-Protocol Translation (NAT-PT)," RFC 2766,

February 2000.

[13] Kivinen, T. et. al., "Negotiation of NAT-Traversal in the IKE," Internet Draft, <draft-ietf-ipsec-nat-t-ike-07.txt>, September 2003.

[14] K. Tsuchiya, H. Higuchi, and Y. Atarashi, "Dual Stack Hosts using the 'Bump-In-the-Stack' Technique (BIS)," RFC 2767, February 2000.

[15] S. Lee, M. Shin, Y. Kim, E. Nordmark, and A. Durand, "Dual Stack Hosts Using 'Bump In the API' (BIA)," RFC 3338, October 2002.

[16] J. Hagino, and K. Yamamoto, "An IPv6-to-IPv4 Transport Relay Translator," RFC 3053, June 2001.

[17] H. Kitamura, "A SOCKS-based IPv6/IPv4 Gateway Mechanism," RFC 3089, April 2001.

[18] J. Soininen, A. Durand and et al., "Transition Scenarios for 3GPP Networks," RFC 3574, August 2003.

[19] C. Huitema, R. Austein, S. Satapati, R. van, "Unmanaged Networks IPv6 Transition Scenarios," Internet Draft, <draft-ietf-v6ops-unman-scenarios-03.txt>, October 2003.

[20] M. Lind, V. Ksinant, D. Park, A. Baudot, "Scenarios and Analysis for Introducing IPv6 into ISP Networks," Internet Draft, <draft-ietf-v6ops-isp-scenarios-analysis-00.txt>, December 2003.

[21] J. Bound, et al., "IPv6 Enterprise Network Scenarios," Internet Draft, <draft-ietf-v6ops-ent-scenarios-00.txt>, October 2003.

◐ 저 자 소 개 ◑

이 희 철

1995년 경북대학교 컴퓨터공학과 (BS)
1997년 경북대학교 컴퓨터공학과 (MS)
2001년 경북대학교 컴퓨터공학과 (Ph.D)
2001년~2002년 ㈜아이투소프트 기술연구소 NGI팀장
2002년~현재 : 한국전자통신연구원 선임연구원
관심분야 : IPv6, IPv4/IPv6 Transition, Mobile IPv6, Wireless Ad-hoc Network

김 형 준

1986년 광운대학교 컴퓨터공학과 (BS)
1988년 광운대학교 컴퓨터공학과 (MS)
1988년~현재 : 한국전자통신연구원 책임연구원/차세대인터넷표준연구팀 팀장
2003년~현재 : 충남대학교 컴퓨터과학과 박사과정 수료
2003년~현재 : IPv6 포럼 코리아 Director
2003년~현재 : ANF(첨단망기술협회) Network Technology Area Director
2002년~현재 : TTA IPv6 전담반 의장
관심분야 : IPv4/IPv6 Transition, Mobile IPv6, Wireless Ad-hoc Network