IPv6/IPv4 통합망에서 IPv4 호스트로부터 IPv6 호스트로의 투명한 연결을 지원하는 4to6 DSTM 구조

준회원 박 은 영*, 종신회원 이 재 훈**

A 4to6 DSTM Architecture Supporting Transparent Connections from IPv4 Hosts to IPv6 Hosts in Integrated IPv6/IPv4 Networks

Eun-young Park* *Associate Member*, Jae-hwoon Lee** *Life Members*

요 약

현재 Internet Protocol Version 4(IPv4) 기반의 인터넷을 한 순간에 Internet Protocol Version 6(IPv6)로 전환하는 것은 불가능하며, 전환 기간 동안에는 두 프로토콜이 공존할 것으로 예상된다 Internet Engineering Task Force(IETF)의 Next Generation Transition Working Group(Ngtrans WG)을 중심으로 많은 전환 메커니즘이 제안되었다. 그러나 대부분의 전환 메커니즘들은 IPv6 망에 있는 호스트로부터 IPv4 망에 있는 호스트로 연결을 설정하는 경우에만 연결을 지원하며, IPv4 망에 있는 호스트가 IPv6 망에 있는 호스트로 연결을 시도하는 경우에는 연결을 지원하지 못하는 문제점을 가지고 있다. 본 논문에서는 IPv4 망에 존재하는 IPv4 클라이언트가 IPv6 망에 존재하는 듀얼 스택 서버로 연결을 설정하고자 하는 경우에 IPv4 클라이언트와 IPv6 망 내의 듀얼 스택 서버 사이에 투명한 연결을 지원하는 IPv4-to-IPv6 듀얼 스택 전환 메커니즘(IPv4-to-IPv6 Dual Stack Transition Mechanism-4to6 DSTM)을 제안한다.

Key Words : IPv4, IPv6, IPv6 Transition Mechanism, IPv4-to-IPv6 Dual Stack Transition Mechanism

ABSTRACT

It is impossible to replace overnight the present Internet Protocol Version 4(IPv4)-based Internet with Internet Protocol Version 6(IPv6). These two protocols are expected to coexist for a number of years during the transition period. A number of transition mechanisms are proposed by Internet Engineering Task Force(IETF) Next Generation Transition Working Group(Ngtrans WG). However, most of them provide only the mechanism to initiate sessions from hosts within the IPv6 network to those within the IPv4 network, but do not support the initiation from IPv4 hosts to IPv6 ones. In this paper, we propose the IPv4-to-IPv6 Dual Stack Transition Mechanism(4to6 DSTM) which can operate even in the case that IPv4 clients in the IPv4 network initiate connections with dual stack servers in the IPv6 network.

Ⅰ. 서 론

현재 Internet Protocol Version 4(IPv4) 기반의 인터넷은 호스트의 급격한 증가로 인한 주소 고갈의 문제와 복잡한 헤더 구조로 인한 라우터의 처리 속도 지연의 문제점을 가지고 있다. 이러한 문제점

* 동국대학교 정보통신공학과(eypark@dongguk.edu), ** 동국대학교 정보통신공학과(jaehwoon@dongguk.edu), 교신저자
논문번호 : 040115-0311, 접수일자 : 2004년 3월 31일
※본 연구는 삼성전자 및 한국과학재단 (R01-2003-000-10628-0) 지원에 의해 수행되었습니다.

을 해결하기 위하여 새로운 인터넷 프로토콜인 Internet Protocol Version 6(IPv6)가 정의 되었다[1][2]. IPv6는 128 비트의 확장된 주소 체계와 단순화된 헤더 구조, 그리고 향상된 QoS 와 이동성, 보안 등의 기능을 가지고 있다. 그러나 현재의 IPv4 중심의 인터넷을 한 순간에 IPv6로 전환하는 것은 불가능하며, 당분간은 IPv4 망과 IPv6 망이 공존하면서 점차적으로 IPv6 망으로 전환될 것이다. 따라서 IPv4에서 IPv6로 인터넷이 성공적으로 전환되기 위해서는 IPv6 노드가 현재 넓게 구축되어 있는 IPv4 노드와 통신할 수 있도록 하는 메커니즘이 필수적이다. 이와 같이 IPv6 망과 IPv4 망이 혼재된 IPv6/IPv4 통합망에서 통신이 자유롭게 이루어 질 수 있도록 하기 위하여 Internet Engineering Task Force(IETF) Next Generation Transition Working Group(Ngtrans WG)을 중심으로 여러 가지 전환 메커니즘들이 제안되었다[3-12]. 그러나 대부분의 전환 메커니즘들은 IPv6 망에 있는 호스트로부터 IPv4 망에 있는 호스트로 연결을 설정하는 경우만을 고려하고 있으며, IPv4 망에 있는 호스트로부터 IPv6 망에 있는 호스트로 연결을 설정하는 경우에는 연결을 지원하지 못하는 문제점을 가지고 있다.

Network Address Translation-Protocol Translation(NAT-PT)는 NAT의 동적 주소 변환 기술과 Statlees IP/ICMP Translation(SIIT)[4]의 프로토콜 변환 기술(즉, 헤더 변환 기술)을 통하여 IPv6 호스트와 IPv4 호스트 사이에서 상호 통신을 가능하게 하는 전환 메커니즘이다[5]. NAT-TP 메커니즘은 IPv4 주소 풀을 이용하여 IPv6 호스트에게 IPv4 주소를 내부적으로 동적 할당하고, IPv6 호스트의 IPv6 주소와 할당한 IPv4 주소에 대한 매핑 정보를 매핑 테이블에 유지한다. NAT-PT 메커니즘은 매핑 테이블의 정보를 이용하여 NAT-PT 변환기를 통과하는 IPv6 패킷을 IPv4 패킷으로 또는 IPv4 패킷을 IPv6 패킷으로 변환한다. 그러나 NAT-PT 메커니즘은 IPv6 패킷을 IPv4 패킷으로 또는 IPv4 패킷을 IPv6 패킷으로 변환하기 때문에, 응용 계층 프로토콜이 자신의 데이터에 IP 주소를 포함하는 경우에는 변환을 지원하지 못하며, 이러한 응용 계층 프로토콜을 수용하기 위해서는 해당 응용 계층 프로토콜에 대한 응용 계층 게이트웨이(Application Level Gateway-ALG)를 가지고 있어야 하는 문제점을 가지고 있다. 또한 NAT-PT 메커니즘은 네트워크 계층과 전송계층에서의 종단간(End-to-End) 보안을 지원할 수 없다.

Dual Stack Transition Mechanism(DSTM)은 IPv6 망 내에 존재하는 듀얼 스택 호스트(즉, DSTM 호스트)가 외부의 IPv4 망에 존재하는 호스트(즉, IPv4 호스트)와 통신할 수 있도록 하는 메커니즘이다[8]. DSTM 호스트는 IPv4 호스트와 통신하고자 하는 경우에 DSTM 서버에게 IPv4 주소를 할당해 줄 것을 요청한다. DSTM 서버는 DSTM 호스트에게 임시의 IPv4 주소와 DSTM Tunnel End-Point(TEP)의 IPv6 주소를 할당한다. DSTM 호스트는 할당받은 IPv4 주소를 이용하여 IPv4 패킷을 만들고, 또한 DSTM TEP의 IPv6 주소를 이용하여 IPv4 패킷을 캡슐화한 후, IPv4-over-IPv6 터널링을 이용하여 DSTM TEP에게로 전송한다. DSTM TEP는 DSTM 호스트로부터 터널링된 패킷을 수신하면 DSTM 호스트의 IPv4 주소와 IPv6 주소에 대한 매핑 정보를 저장하고 터널링된 패킷을 디캡슐레이션한 후 IPv4 망으로 전송한다. DSTM TEP는 IPv4 호스트로부터 DSTM 호스트로 전송되는 IPv4 패킷을 수신하면 저장된 매핑 정보를 이용하여 캡슐화한 후 터널링 메커니즘을 이용하여 DSTM 호스트로 전송한다. DSTM 메커니즘은 터널링 방법을 통하여 듀얼 스택 호스트와 IPv4 호스트 사이에 투명한 경로를 제공하기 때문에, NAT-PT 메커니즘과 같이 프로토콜 변환에 의한 문제점을 가지지 않는다는 장점이 있다. 그렇지만 기존의 DSTM 메커니즘은 IPv6 망에 있는 듀얼 스택 호스트에서 IPv4 망에 있는 IPv4 호스트로 연결을 설정하는 경우에만 연결을 지원하며, IPv4 망 내의 IPv4 호스트에서 IPv6 망 내의 듀얼 스택 호스트로 연결을 설정하는 경우에는 연결을 지원하지 못하는 문제점을 가지고 있다.

따라서 본 논문에서는 IPv4 망에 존재하는 IPv4 호스트가 IPv6 망에 존재하는 듀얼 스택 호스트로 연결을 설정하는 경우에 IPv4 호스트와 듀얼 스택 호스트 사이에 투명한 연결을 제공하는 IPv4-to- IPv6 듀얼 스택 전환 메커니즘 (IPv4-to-IPv6 Dual Stack Transition Mechanism-4to6 DSTM)을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 본 논문에서 제안하는 4to6 DSTM 메커니즘의 동작과 구조에 대해서 자세히 설명하고, 3 장에서는 모의실험을 통하여 제안 메커니즘의 동작과 성능을 분석한다. 그리고 마지막으로 4 장에서 결론을 맺는다.

Ⅱ. 4to6 DSTM 메커니즘

2.1 4to6 DSTM 메커니즘의 구조 및 동작원리

제안된 4to6 DSTM 메커니즘의 구조 및 동작 원리는 그림 1에 나타나 있다. 4to6 DSTM 메커니즘은 DSTM 서버, DSTM TEP, 그리고 듀얼 스택의 DSTM 호스트로 구성된다. DSTM 서버는 DSTM 호스트에게 임시의 IPv4 주소를 할당하고, 할당한 IPv4 주소와 DSTM 호스트의 IPv6 주소에 대한 매핑 테이블을 유지한다. DSTM TEP는 IPv6 망과 IPv4 망의 경계에 위치하면서 IPv4 패킷을 DSTM 호스트로 터널링한다.

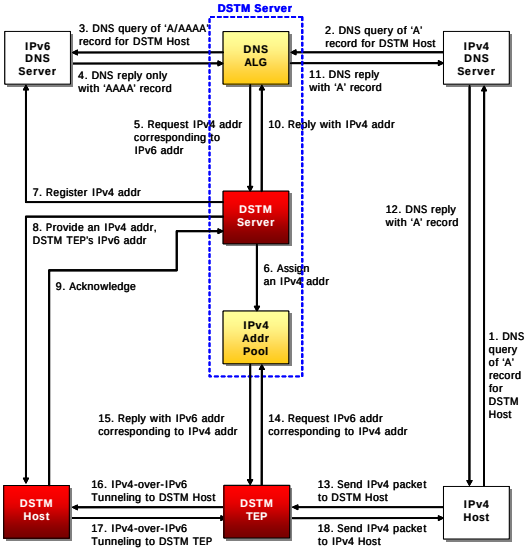


그림 1. 4to6 DSTM 메커니즘의 구조 및 동작 원리

IPv4 호스트가 DSTM 호스트와 연결을 설정하기 위해서는 DSTM 호스트의 IPv4 주소를 알아야 한다. 일반적으로 IPv4 호스트는 IPv4 망 내에 있는 IPv4 Domain Name System(DNS) 서버에게 DSTM 호스트의 IPv4 주소를 묻는 A 타입(A: IPv4 주소에 대한 DNS 레코드 타입)의 DNS 질의 메시지를 전송한다. IPv4 DNS 서버는 DSTM 호스트에 대한 DNS 정보를 가지고 있지 않기 때문에, 해당 정보를 가지고 있는 IPv6 망 내의 IPv6 DNS 서버로 DNS 질의 메시지를 전송한다. IPv4 DNS 서버가 전송한 DNS 질의 메시지는 IPv6 망과 IPv4 망의 경계에 존재하는 DSTM TEP로 전송된다. DSTM TEP는 수신한 DNS 질의 메시지의 목적지 주소를 보고 IPv6 DNS 서버로 전송되는 패킷임을 알 수 있다. DSTM TEP는 수신한 DNS 질의 메시지를 DSTM 서버로 전송한다. DSTM 서버는 DNS-ALG[13]를 통하여 수신한 A 타입의 DNS 질의 메시지를 IPv4 주소 정보와 IPv6 주소 정보를 모두 요청하는 A/AAAA 타입(AAAA: IPv6 주소에 대한 DNS 레코드 타입)의 DNS 질의 메시지로 변환하여 IPv6 DNS 서버로 전송한다. DSTM 서버는 IPv6 DNS 서버로부터 DSTM 호스트의 IPv4 주소와 IPv6 주소 정보를 모두 포함하는 A/AAAA 타입의 DNS 응답 메시지를 수신하면, DNS-ALG를 이용하여 수신한 A/AAAA 타입의 DNS 응답 메시지를 IPv4 주소 정보만을 포함하는 A 타입의 DNS 응답 메시지로 변환한다. 그리고 DSTM 서버는 A 타입의 DNS 응답 메시지를 IPv4 DNS 서버로 전송한다. 만약 DSTM 서버가 IPv6 DNS 서버로부터 DSTM 호스트의 IPv6 주소 정보만을 포함하는 AAAA 타입의 DNS 응답 메시지를 수신하면, DSTM 서버는 자신의 IPv4 주소 풀(IPv4 address pool)로부터 임시의 IPv4 주소 하나를 DSTM 호스트에 할당한다. DSTM 서버는 자신의 매핑 테이블에 DSTM 호스트의 IPv6 주소와 할당한 IPv4 주소, 그리고 할당한 IPv4 주소가 유효하게 사용될 수 있는 시간을 나타내는 lifetime 등의 매핑 정보를 저장하고 lifetime에 대한 타이머를 설정한다. 그리고 DSTM 서버는 할당한 IPv4 주소 정보를 IPv6 DNS 서버에 동적으로 등록한다[14]. DSTM 서버는 DSTM 호스트로 DSTM 주소 할당 메시지(DSTM Address Allocation Message)를 전송하여 할당한 IPv4 주소와 터널링에 사용될 DSTM TEP의 IPv6 주소 정보, 그리고 lifetime 등의 정보를 알려준다. DSTM 호스트는 DSTM 서버로부터 DSTM 주소 할당 메시지를 수신하면, 할당 받은 IPv4 주소와 DSTM TEP의 IPv6 주소를 캐쉬에 저장하고 lifetime에 대한 타이머를 설정한다. 그리고 DSTM 호스트는 DSTM 서버로 DSTM 주소 할당 응답 메시지(DSTM Address Allocation Aacknowledgement Message)를 전송하여 주소 할당이 성공적으로 처리되었음을 알려준다. DSTM 서버는 DSTM 호스트로부터 DSTM 주소 할당 응답 메시지를 수신하면, DNS-ALG를 통하여 IPv6 DNS 서버로부터 수신한 AAAA 타입의 DNS 응답 메시지를 할당한 IPv4 주소 정보를 포함하는 A 타입의 DNS 응답 메시지로 변환한다. 그리고 DSTM 서버는 A 타입의 DNS 응답 메시지를 IPv4 DNS 서버로 전송한다. IPv4 DNS 서버는 IPv4 호스트에게 수신한 DNS 응답

메시지를 전송한다.

IPv4 호스트는 수신한 DNS 응답 메시지로부터 얻은 DSTM 호스트의 IPv4 주소를 이용하여 DSTM 호스트로 IPv4 패킷을 전송한다. IPv4 호스트로부터 전송된 IPv4 패킷은 IPv6 망과 IPv4 망의 경계에 존재하는 DSTM TEP로 전송된다. DSTM TEP는 IPv4 호스트로부터 전송된 IPv4 패킷을 수신하면, 자신의 매핑 테이블을 조사하여 수신한 IPv4 패킷의 목적지 주소에 매핑되는 IPv6 주소 정보(즉, 해당 DSTM 호스트의 IPv6 주소)가 있는지 검사한다. 만약 DSTM TEP가 해당 매핑 정보를 가지고 있다면, DSTM TEP는 해당 매핑 정보를 이용하여 수신한 IPv4 패킷을 IPv6 패킷에 인캡슐레이션하고 IPv4-over-IPv6 터널링을 이용하여 DSTM 호스트로 전송한다. 만약 DSTM TEP가 수신한 IPv4 패킷의 목적지 주소에 대한 IPv6 주소 정보를 가지고 있지 않다면, DSTM TEP는 DSTM 서버에게 DSTM 바인딩 요청 메시지(DSTM Binding Request Message)를 전송하여 수신한 IPv4 패킷의 목적지 주소에 대한 IPv6 주소 정보를 포함하는 매핑 정보를 전송해 줄 것을 요청한다. DSTM 서버는 DSTM TEP로부터 DSTM 바인딩 요청 메시지를 수신하면, 자신의 매핑 테이블을 조사하여 요청한 IPv4 주소에 대한 IPv6 주소 정보를 포함하는 매핑 엔트리를 찾아 DSTM 바인딩 갱신 메시지(DSTM Binding Update Message)를 통하여 DSTM TEP에게 매핑 정보를 전송한다. DSTM TEP는 DSTM 서버로부터 DSTM 바인딩 갱신 메시지를 수신하면, 자신의 매핑 테이블에 DSTM 호스트의 IPv4 주소와 IPv6 주소, 그리고 매핑 정보가 유효하게 사용될 수 있는 시간을 나타내는 lifetime 등의 정보를 저장하고 lifetime에 대한 타이머를 설정한다. DSTM TEP는 저장한 매핑 정보를 이용하여 IPv4 호스트로부터 수신한 IPv4 패킷을 DSTM 호스트로 IPv4-over-IPv6 터널링한다. DSTM 호스트는 DSTM TEP로부터 터널링된 패킷을 수신하면, 디캡슐레이션하여 IPv4 호스트가 전송한 원본의 IPv4 패킷을 수신할 수 있다. DSTM 호스트는 할당받은 IPv4 주소와 DSTM TEP의 IPv6 주소를 이용하여 DSTM TEP로 IPv4 패킷을 IPv4-over-IPv6 터널링하고, 이를 DSTM TEP가 디캡슐레이션하여 IPv4 망으로 전송한다.

DSTM 서버는 자신의 매핑 테이블의 각 엔트리마다 설정해 놓은 타이머가 만료되면(즉, DSTM 호스트에게 할당한 IPv4 주소에 대한 lifetime이 지나면), 매핑 테이블에서 해당 엔트리를 삭제한다. 그리고 DSTM 서버는 IPv6 DNS 서버로부터 IPv4 주소 할당 시에 등록했던 DSTM 호스트의 IPv4 주소 정보를 삭제하고, DSTM 호스트에게서 할당했던 IPv4 주소를 회수한다. DSTM 호스트는 자신이 할당받은 IPv4 주소를 lifetime 이후에도 계속 사용하기 위해서는 lifetime 만료전에 DSTM 서버로 DSTM 주소 연장 요청 메시지(DSTM Address Extension Request Message)를 전송하여 할당 받은 IPv4 주소의 lifetime을 연장해야 한다. DSTM 서버는 DSTM 호스트로부터 DSTM 주소 연장 메시지를 수신하면, 매핑 테이블에서 해당 엔트리를 찾아 lifetime을 연장하고 해당 타이머를 재설정한다. 그리고 DSTM 서버는 DSTM 호스트에게 DSTM 주소 연장 응답 메시지(DSTM Address Extension Acknowledgement Message)를 전송한다. DSTM TEP는 자신의 매핑 테이블의 각 엔트리마다 설정해 놓은 타이머가 만료할 때까지 해당 매핑 정보의 사용이 없으면 매핑 테이블에서 해당 엔트리를 삭제한다. 그리고 DSTM TEP는 타이머가 만료되기 전에 해당 매핑 정보가 사용된 경우에는 타이머 만료전에 DSTM 서버에게 DSTM 바인딩 요청 메시지(DSTM Binding Request Message)를 전송하여 매핑 정보를 갱신하고 해당 타이머를 재설정한다.

2.2 DSTM 메시지의 정의

이 절에서는 제안한 4to6 DSTM 메커니즘에서 DSTM 서버와 DSTM 호스트 간에 IPv4 주소 할당을 위하여 필요한 DSTM 메시지와 DSTM 서버와 DSTM TEP간에 바인딩 정보 갱신을 위하여 필요한 DSTM 메시지를 정의한다. 4to6 DSTM 메커니즘은 UDP 위에서 그림 2에 정의된 것과 같은 DSTM 메시지를 이용하여 동작한다.

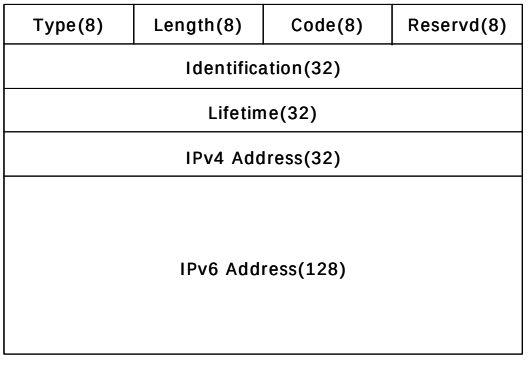


그림 2. DSTM 메시지의 형식

Type 필드는 DSTM 메시지의 타입을 나타내며, Length 필드는 바이트 단위의 DSTM 메시지 길이를 나타낸다. Code 필드는 DSTM 메시지의 처리 결과를 표시하기 위해서 사용되고, Identification 필드는 DSTM 요청 메시지와 응답 메시지의 일치를 위하여 사용되는 식별자이다. Lifetime 필든 IPv4 Address 필드와 IPv6 Address 필드의 정보가 유효하게 사용될 수 있는 시간을 나타낸다. IPv4 Address 필드는 DSTM 호스트의 IPv4 주소를 나타내고, IPv6 Address 필드는 DSTM 호스트의 IPv6 주소 또는 DSTM TEP의 IPv6 주소를 위해 사용된다.

2.2.1 DSTM 주소 할당 요청 메시지

DSTM 호스트가 IPv4 호스트로 연결을 설정하는 경우에 DSTM 호스트는 DSTM 서버에게 IPv4 주소를 할당해 줄 것을 요청한다. DSTM 주소 할당 요청 메시지는 DSTM 호스트가 DSTM 서버에게 IPv4 주소를 할당해 줄 것을 요청하기 위하여 사용되는 DSTM 메시지이다. IPv4 Address 필드는 0으로 설정하고, IPv6 Address 필드는 IPv4 주소 할당을 요청하는 DSTM 호스트의 IPv6 주소를 기입한다.

2.2.2 DSTM 주소 할당 메시지

DSTM 주소 할당 메시지는 DSTM 서버가 DSTM 호스트에게 IPv4 주소를 할당하기 위하여 사용되는 DSTM 메시지이다. IPv4 Address 필드는 할당한 IPv4 주소를 기입하고, IPv6 Address 필드에는 터널링에 사용될 DSTM TEP의 IPv6 주소를 기입한다.

2.2.3 DSTM 주소 할당 응답 메시지

DSTM 주소 할당 응답 메시지는 DSTM 호스트가 DSTM 서버에게 DSTM 주소 할당 메시지의 처리 결과를 알려주기 위하여 사용되는DSTM 메시지이다. IPv4 Address 필드에는 DSTM 서버로부터 할당받은 IPv4 주소를 기입하고, IPv6 Address 필드에는 DSTM 호스트의 IPv6 주소를 기입한다.

2.2.4 DSTM 주소 연장 요청 메시지

DSTM 주소 연장 요청 메시지는 DSTM 호스트가 DSTM 서버에게 할당 받은 IPv4 주소의 lifetime을 연장해 줄 것을 요청하기 위하여 사용되는 DSTM 메시지이다. IPv4 Address 필드에는 DSTM 서버로부터 할당받은 IPv4 주소를 기입하고, IPv6 Address 필드에는 DSTM 호스트의 IPv6 주소를 기입한다.

2.2.5 DSTM 주소 연장 메시지

DSTM 주소 연장 메시지는 DSTM 서버가 DSTM 호스트에게 DSTM 주소 연장 요청 메시지에 대한 처리 결과를 알려주기 위하여 사용되는 DSTM 메시지이다. IPv4 Address 필드는 연장되어서 사용될 수 있는 IPv4 주소를 기입하고, IPv6 Address 필드는 터널링에 사용될 DSTM TEP의 IPv6 주소를 기입한다.

2.2.6 DSTM 바인딩 요청 메시지

DSTM 바인딩 요청 메시지는 DSTM TEP가 DSTM 서버에게 DSTM 호스트에 대한 매핑 정보를 요청하기 위하여 사용되는 DSTM 메시지이다. IPv4 Address 필드는 DSTM 호스트의 IPv4 주소를 기입하고, IPv6 Address 필드에는 매핑 정보를 요청하는 DSTM TEP의 IPv6 주소를 기입한다.

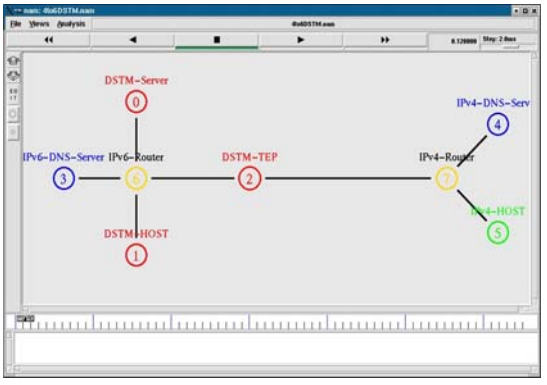
2.2.7 DSTM 바인딩 갱신 메시지

DSTM 바인딩 갱신 메시지는 DSTM 서버가 DSTM TEP에게 DSTM 호스트에 대한 매핑 정보를 전송하기 위하여 사용되는 DSTM 메시지이다. IPv4 Address 필드와 IPv6 Address 필드는 DSTM 호스트의 IPv4 주소와 IPv6 주소를 기입한다.

Ⅲ. 성능평가

이 장에서는 모의실험을 통하여 제안한 4to6 DSTM 메커니즘의 동작과 성능을 분석한다. 모의실험은 네트워크 시뮬레이터 ns-2를 사용하였다[15]. 모의실험을 위한 모델과 각 노드들 사이의 링크의 전송 속도 및 지연 시간은 그림 3에 나타나 있다. 모의실험에서는 IPv4 호스트가 DSTM 호스트에 대한 DNS 질의 메시지를 전송하여 DSTM 호스트에 대한 IPv4 주소 정보를 얻고, DSTM 호스트로 IPv4 패킷을 전송함으로써 DSTM 호스트와 연결을 설정하는 경우를 모의실험 한다.

그림 4는 20개의 IPv4 호스트가 DSTM 호스트로 연결을 설정하기 위하여 2초 간격으로 DSTM 호스트에 대한 DNS 질의 메시지를 전송하는 경우에, IPv4 호스트로부터 전송된 DNS 질의 메시지에 대한 DNS 응답 시간을 보여준다. DNS 응답 시간은 IPv4 호스트가 DNS 질의 메시지를 전송한 시간부터 IPv4 호스트가 DNS 응답 메시지를 수신하기까지 걸린 시간으로 정의한다. 첫 번째 IPv4 호스트



DSTM Server – IPv6 Router : 10Mb, 20ms
IPv6 DNS Sever – IPv6 Router : 10Mb, 20ms
DSTM Host – IPv6 Router : 10Mb, 20ms
IPv6 Router – DSTM TEP : 10Mb, 40ms
DSTM TEP – IPv4 Router : 10Mb, 80ms
IPv4 DNS Server – IPv4 Router : 10Mb, 20ms
IPv4 Host – IPv4 Router : 10Mb, 20ms

그림 3. 모의실험 모델

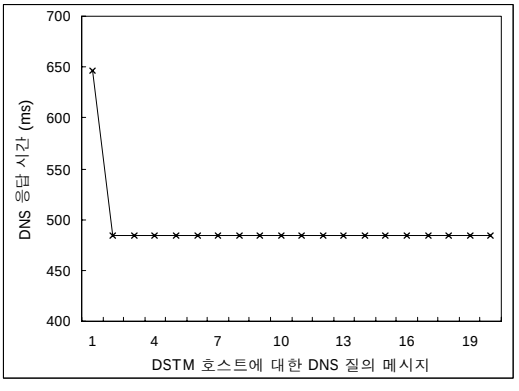


그림 4. DNS 응답시간

가 DSTM 호스트에 대한 DNS 질의 메시지를 전송한 경우에, DSTM 서버는 DSTM 호스트에게 IPv4 주소를 할당하고, IPv6 DNS 서버에 할당한 IPv4 주소 정보를 등록해야 한다. 또한 DSTM 서버는 DSTM 호스트에게 DSTM 주소 할당 메시지를 전송하여 할당한 IPv4 주소와 터널링에 사용할 DSTM TEP의 IPv6 주소를 알려주는 것이 필요하다. 이로 인하여 첫 번째 IPv4 호스트로부터 전송된 DNS 질의 메시지는 큰 DNS 응답 시간을 갖고, 그 이후에 전송된 DNS 질의 메시지는 DSTM 호스트가 IPv4 주소를 가지고 있으며 IPv6 DNS 서버가 DSTM 호스트에 대한 IPv4 주소 정보를 가지고 있기 때문에, IPv4 주소 할당과 DNS 등록 절차를 거치지 않아 처음 전송된 DNS 질의 메시지보다 작은 DNS 응답 시간을 갖는 것을 볼 수 있다.

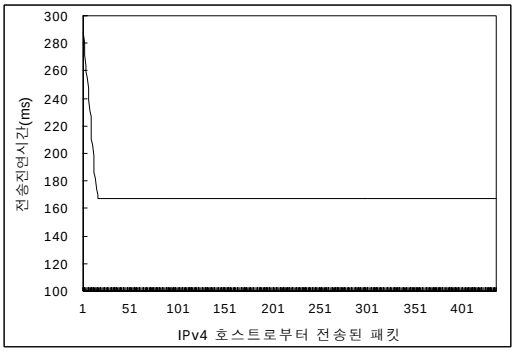


그림 5. 전송지연시간

그림 5는 IPv4 호스트가 DNS 질의 메시지를 통하여 DSTM 호스트의 IPv4 주소를 알고 난 후에 DSTM 호스트로 IPv4 패킷을 전송하는 경우에, IPv4 호스트로부터 DSTM 호스트로 전송된 패킷이 겪는 전송지연시간을 보여준다. DSTM TEP가 IPv4 호스트로부터 전송된 IPv4 패킷을 처음 수신하면, DSTM TEP는 자신의 매핑 테이블에 DSTM 호스트에 대한 매핑 정보를 가지고 있지 않기 때문에, DSTM 서버에게 매핑 정보를 요청하는 DSTM 바인딩 요청 메시지를 전송하고 DSTM 서버로부터 DSTM 바인딩 갱신 메시지를 수신하는 것이 필요하다. 이로 인하여 그림 5에서와 같이 IPv4 호스트로부터 처음 전송된 패킷은 큰 전송지연시간을 갖고, 그 이후로 전송된 패킷들은 DSTM TEP가 DSTM 호스트에 대한 매핑 정보를 가지고 있기 때문에 DSTM 서버에게 매핑 정보를 요청하는 절차를 필요로 하지 않아 처음 전송된 패킷보다 작은 전송지연을 겪는 것을 볼 수 있다

그림 6은 1000개의 IPv4 호스트가 DSTM 호스트에 대한 DNS 질의 메시지를 전송함으로써 DSTM 호스트로 연결을 시도하는 경우에 IPv4 호스트가 DSTM 호스트로 연결을 시도하는 평균 간격에 따라 IPv4 호스트로부터 전송된 DNS 질의 메시지에 대한 평균 DNS 응답 시간을 보여준다. IPv4 호스트가 DSTM 호스트로 연결을 시도하는 간격(평균: 2초, 4초, 6초, 8초, 10초)과 IPv4 호스트가 DSTM 호스트와 연결을 지속하는 시간(평균: 4초, 6초, 8초)은 지수분포를 사용하였다. DSTM 호스트는 IPv4 호스트와 통신이 끝나면 할당 받은 IPv4 주소를 DSTM 서버에게 반납하고, DSTM 서버는 회수한 IPv4 주소에 대한 DNS 정보를 IPv6 DNS 서버로부터 삭제한다. 따라서 DSTM 호스트와 IPv4 호스트 사이에 통신 끝난 이후에 새로운

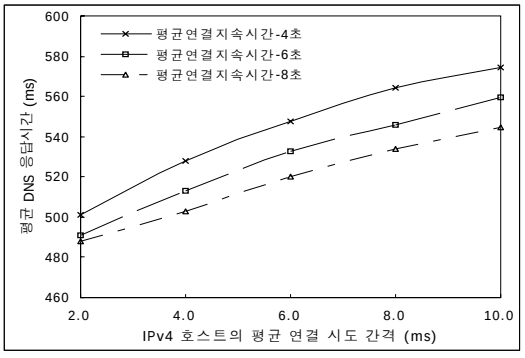


그림 6. 평균 DNS 응답시간

IPv4 호스트가 DSTM 호스트로 연결을 시도하면, DSTM 서버는 DSTM 호스트에게 IPv4 주소를 재할당하고, 할당한 IPv4 주소 정보를 IPv6 DNS 서버에 재등록해야 한다. 따라서 IPv4 호스트가 DSTM 호스트와 연결을 지속하는 시간보다 IPv4 호스트가 DSTM 호스트로 연결을 시도하는 간격이 더 크면, IPv4 호스트가 DSTM 호스트로 연결을 시도할 때 마다 DSTM 서버는 반복해서 DSTM 호스트에게 IPv4 주소를 할당하고, 할당한 IPv4 주소 정보를 IPv6 DNS 서버에 등록해야 하기 때문에 DNS 응답시간이 커진다. 그림 6에서와 같이 IPv4 호스트가 DSTM 호스트로 연결을 시도하는 간격이 클수록, 그리고 IPv4 호스트가 DSTM 호스트와 연결을 지속하는 시간이 작을수록 큰 DNS 응답시간을 가지는 것을 볼 수 있다.

Ⅳ. 결 론

현재의 IPv4 기반의 인터넷은 호스트의 급격한 증가로 인한 주소 고갈의 문제와 복잡한 헤더 구조로 인한 라우터의 처리 속도 지연의 문제점을 가지고 있다. 이러한 문제점을 해결하기 위하여 새로운 인터넷 프로토콜인 IPv6가 정의 되었다. 그러나 현재의 IPv4 중심의 인터넷을 한 순간에 IPv6로 전환하는 것은 불가능하며, 전환 기간 동안에는 두 프로토콜이 공존할 것으로 예상된다. IETF Ngtrans WG을 중심으로 많은 전환 메커니즘이 제안되었다. 그러나, 대부분의 전환 메커니즘들은 IPv6 망에 있는 호스트로부터 IPv4 망에 있는 호스트로 연결을 설정하는 경우에만 연결을 지원하며, IPv4 망에 있는 호스트가 IPv6 망에 있는 호스트로 연결을 설정하는 경우에는 연결을 지원하지 못하는 문제점을 가지고 있다.

본 논문에서는 IPv4 망에 존재하는 IPv4 호스트(즉, 클라이언트)가 IPv6 망에 존재하는 듀얼 스택 호스트(즉, 서버)로 연결을 설정하는 경우에 IPv4 호스트와 IPv6 망 내의 듀얼 스택 호스트 사이에 투명한 연결 지원하는 4to6DSTM 메커니즘을 제안하였다.

제안된 4to6 DSTM 메커니즘의 동작 및 성능은 ns-2 기반의 모의실험을 통하여 분석되었다. 모의실험의 결과, 그림 4와 5에 나타난 것과 같이 IPv4 망에 존재하는 IPv4 호스트가 IPv6 망에 존재하는 듀얼 스택 호스트로 연결을 설정하고자 하는 경우에, 듀얼 스택 호스트에 동적으로 IPv4 주소를 할당함으로써 듀얼 호스트와 IPv4 호스트 사이에 투명한 연결을 지원하는 것을 볼 수 있었다. 또한 그림 6에 나타난 것과 같이 IPv4 호스트가 IPv6 망에 존재하는 듀얼 스택 호스트에 대한 DNS 질의 메시지를 전송함으로써 듀얼 스택 호스트로 연결을 설정하는 경우에, IPv4 호스트가 듀얼 스택 호스트로 연결을 시도하는 간격과 IPv4 호스트가 듀얼 스택 호스트와 연결을 지속하는 시간에 따라 DNS 응답 시간이 달라지는 것을 볼 수 있었다.

참 고 문 헌

[1] S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” Internet Engineering Task Force RFC 2460, December 1998; http://www.ietf.org/rfc/rfc2460.txt.

[2] R. Hinden, S. Deering, “IP Version 6 Addressing Architecture,” Internet Engineering Task Force RFC 3513, April 2003; //www.ietf.org/rfc/rfc3513.txt.

[3] R. Gilligan, E. Nordmark, “Transition Mechanisms for IPv6 hosts and Routers,” Internet Engineering Task Force RFC 2893, August 200; www.ietf.org/rfc/rfc2893.txt.

[4] E, Nordmark, “Stateless IP/ICMP Translation Algorithm (SIIT)”, Internet Engineering Task Force RFC 2765, February 2000; www.ietf.org/rfc/rfc2766.txt.

[5] G. Tsirtsis, P. Srisuresh, “Network Address Translation Protocol Translation (NAT-PT),” Internet Engineering Task Force RFC 2766, February 2000; www.ietf.org/rfc/rfc2766.txt.

[6] H. Kitamura, “A SOCKS-based IPv6/IPv4

Gateway Mechanism," Internet Engineering Task Force RFC 3089, April 2001; //www.ietf.org/rfc/rfc3081.txt.

[7] J. Hagino, K. Yamamoto, "An IPv6-to-IPv4 Transport Relay Translator," Internet Engineering Task Force RFC 3142, June 2001; www.ietf.org/rfc/rfc3142.txt.

[8] J. Bound, L. Toutain, H. Affifi, "Dual Stack Transition Mechanism (DSTM)," Internet Draft, Internet Engineering Task Force, January 2002; work in progress.

[9] K. Tsuchiya, H. Higuchi, Y. Atarashi, "Dual-Stack Hosts Using the 'Bump-In-the-Stack' (BIS) Technique," Internet Engineering Task Force RFC 2767, February 2000; www.ietf.org/rfc/rfc2767.txt.

[10] S. Lee, M. Shin, Y. Lee, "Dual-Stack Hosts Using 'Bump in the API (BIA)," Internet Engineering Task Force RFC 3338, October 2002; www.ietf.org/rfc/rfc3338.txt.

[11] A. Durand, P. Fasano, I. Guardini, D. Lento, "IPv6 Tunnel Broker," Internet Engineering Task Force RFC 3053, January 2001; www.ietf.org/rfc/rfc3053.txt.

[12] B. Carpenter, K. Moore, "Connection of IPv6 Domains via IPv4 Clouds," Internet Engineering Task Force RFC 3056, February 2001; www.ietf.org/rfc/rfc3056.txt.

[13] P. srisuresh, G. Tsirtsis P. Akkiragu, A. Heffernan, "DNS extensions to Network Address Translators (DNS_ALG)," Internet Engineering Task Force RFC 2694, September 1999; www.ietf.org/rfc/rfc2694.txt.

[14] P. Vixie, S. Thomson, Y. Rekhter, J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", Internet Engineering Task Force RFC 2136, April 1997; www.ietf.org/rfc/rfc2136.txt.

[15] LBL, Xerox PARC, UCB, USC/ISI, VINIT Project, The Network Simulator *ns-2* www.isi.edu/nsnam/ns.

박 은 영 (Eun-young Park) 준회원

2001년 2월 동국대학교 정보통신공학과 학사

2004년 2월 동국대학교 정보통신공학과 석사

2004년 3월~현재 LG전자기술원연구원

<관심분야> IPv6, Mobile IP, Routing Protocol, 차세대 인터넷 프로토콜

이 재 훈 (Jae-hwoon Lee) 종신회원

1985년 2월 한양대학교 전자공학과 학사

1987년 2월 한국과학기술원 전기 및 전자공학과 석사

1995년 8월 한국과학기술원 전기 및 전자공학과 박사

1987년 3월~1990년 4월 데이콤 연구원

1990년 9월~1999년 2월 삼성전자 정보통신부문 선임연구원

2000년 3월~2000년 12월 삼성전자 자문교수

1999년 3월~현재 동국대학교 정보통신공학과 조교수

2000년 5월~현재 10G 이더넷포럼 운영위원

<관심분야> 초고속통신, 다중 엑세스 프로토콜, 인터넷 프로토콜, 광 네트워크 프로토콜