IPv4/IPv6 프로토콜 및 주소변환 기능의 요소기술 분석 및 설계

(Analysis and Design of Functional Blocks for IPv4/IPv6 Protocol and Address Translation)

이 승 민 † 진 재 경 †† 민 상 원 †††

(Seung-Min Lee) (Jae-Kyung Jin) (Sang-Won Min)

요 약 기존의 IPv4 문제점을 극복하기 위해 IETF (Internet Engineering Task Force)에서 제안하고 있는 IPv6 (IP version 6)는 초기 도입단계에서 IPv4와의 호환성을 위해 다양한 트랜지션 메커니즘이 필요하다. 이러한 트랜지션 메커니즘은 크게 터널링과 변환기를 이용한 메커니즘으로 구분될 수 있다. 본 논문은 변환기를 이용한 트랜지션 메커니즘 구현을 위해 기존의 NAT (Network Address Translation) 기법과 유사한 NAT-PT (NAT-Protocol Translation) 표준을 기반으로 변환에 필요한 요소 기술들을 분석하였다. 그리고 global IPv4 주소의 효율적인 활용을 위해서 포트를 이용한 확장 알고리즘을 설계하여 제시하였다. 또한 표준에서 언급되지 않은 매핑 테이블 관리 및 타이머 설정, 그리고 구현에 필요한 세부 기술들을 분석하여 설명하였다. 본 논문에서 제시한 모델은 양방향 세션의 NAT-PT 방식과 기존의 포트변환 방식을 혼용한 방식이다. 제안된 방식은 IPv4 주소를 필요로 하는 모든 호스트에 IPv4 주소를 할당하지 않고 단일 임시 IPv4 주소와 포트를 할당하기 때문에 IPv4 주소가 효율적으로 운영할 수 있는 장점을 갖는다.

키워드 : IPv4/IPv6 변환기술, NAT-PT, 주소변환

Abstract IPv6 (IP version 6), which was standardized by the IETF (Internet Engineering Task Force) to cope with existing IPv4 problems, needs several approaches for interoperation with IPv4. The internetworking of IPv6 with IPv4 is an important key to the deployment of the next generation Internet. As the solutions to the transition mechanism, both tunneling and translator methods have been proposed. In this paper, we analyze functional elements for implementation design of a transition mechanism based on the NAT-PT (NAT-Protocol Translation), and propose an extension algorithm that uses ports for effective use of global IPv4 addresses. The algorithm presented in this paper is a method of combining NAT-PT with Port Translation mechanism. The algorithm does not assign an IPv4 address to the host that needs IPv4 address, but allocates a single temporary IPv4 address and a port number in order to identify host.

Key words : IPv4/IPv6 Transition Mechanism, NAT-PT, Address Translation

1. 서 론

현재 IPv4(Internet Protocol version 4) 주소를 이용한 인터넷 환경은 초기 인터넷환경과는 달리 통신기술의 급진적인 발달과 인터넷 사용자 수의 기하급수적인 증가, 그리고 사용자들의 새롭고 다양한 서비스에 대한 요구로 인해 많은 변화가 발생하였다. 기존의 IPv4는 32비트 주소 체계에 따른 클래스 기반의 주소할당 방식 때문에 향후 이동통신의 All IP, 스마트 정보가전 서비

· 이 논문은 2001년도 광운대학교 교내학술 연구비 지원에 의해 수행되었음.

† 비 회 원 : 삼성전자 정보통신총괄 무선사업부 연구원
sminlee@samsung.co.kr
†† 비 회 원 : 모다정보통신 연구원
jkjin93@yahoo.co.kr
††† 정 회 원 : 광운대학교 전자공학부 교수
min@daisy.gwu.ac.kr

논문접수 : 2001년 12월 24일
심사완료 : 2002년 10월 14일

스 등에서 예상되는 주소 수요를 감당하기에는 어려움이 있다. 그리고 IPv4 패킷 헤더의 구조에 따른 멀티캐스팅, 보안기술 등의 서비스 제공에도 많은 문제점이 있다. 이러한 문제점들을 극복하기 위해 IETF (Internet Engineering Task Force)의 IPng(IP next generation) working group에서는 128비트의 주소체계를 가지는 새로운 IPv6(IP version 6) 프로토콜을 권고하였다[1, 2].

IPv6가 비록 이전 버전보다 향상된 기능들을 제공하고 있음에도 불구하고 기존의 IPv4 네트워크를 IPv6 네트워크로 일시에 대체하는 것은 현실적으로 어려움이 있다. 따라서 IPv6의 광범위한 사용 및 완전한 도입 이전까지는 IPv4와의 공존이 예상되기 때문에 IPv6 초기 도입단계에서는 IPv6 네트워크가 기존 IPv4와의 연동 및 호환을 고려하여 구축되어야 한다. 이를 위해 두 네트워크의 연동을 위한 IPv4-to-IPv6의 트랜지션(transition)과 상호공존(coexistence mechanism) 메커니즘이 운영되어야 한다. 이러한 트랜지션 메커니즘은 IETF의 NGTrans(Next generation translation) working group에서 활발한 연구 및 개발이 진행되면서 다양한 기술들이 제안되고 있다. 제안된 메커니즘들은 크게 터널링(tunneling)과 변환기 (translator)를 이용한 메커니즘으로 분류될 수 있다[2~5].

본 논문에서는 이러한 트랜지션 메커니즘 중에서 변환기를 이용한 방식인 IETF의 NAT-PT(Network Address Translation - Protocol Translation) 표준 기본 알고리즘과 global IPv4 주소의 효과적인 활용을 위한 포트 변환 알고리즘을 적용하여 설계하였다. 알고리즘 설계를 위해 변환기 기능을 주소변환과 프로토콜 변환의 기능으로 구분하여 각 변환에 적합한 요소기술들을 분석하였다. 그리고 이를 통해 기존의 NAT 방식을 응용한 NAT-PT 표준 방식의 IPv4/IPv6 변환기 모델을 설계하였다. 본 논문에서 제시한 모델은 NAT-PT 방식과 임시 IPv4 주소를 효율적으로 운영할 수 있도록 하는 아웃바운드(outbound) 세션의 포트 변환 방식의 혼용이 특징이다. 그리고 인바운드(inbound) 세션에 대한 제한을 개선함으로써 FTP, DNS와 같은 애플리케이션의 양방향 세션 설정이 가능하도록 하였다.

본 논문은 이러한 요소 기술들 분석을 위해 서론에 이어 2장에서는 NAT-PT 표준에 대한 소개와 실제 변환 방법인 주소 변환 방법과 개선 알고리즘에 대해 설명하고, 3장에서는 패킷의 프로토콜 변환 방법에 설명한다. 그리고 4장에서는 소개한 두 알고리즘을 기반으로 한 모델의 설계와 각 구성요소별 기능에 대해 설명한 후 5장에서 결론을 맺는다.

2. IPv4/IPv6 주소 변환과 개선 알고리즘

NAT-PT 메커니즘은 변환기가 두 네트워크의 경계에 위치하여 연결이 설정되는 방향에 따라 각 IPv6 네트워크 주소가 정적 또는 동적으로 IPv4 주소들과 결합되는 방식이다. IPv4/IPv6 주소 변환시 IPv6의 128 비트 주소형식은 IPv4의 32비트 주소형식으로 표현할 수 없다. 또한 각 네트워크의 DNS는 다른 RR(resource record)를 운용하기 때문에 IPv4에서 IPv6로의 인바운드 세션의 주소변환에 어려움이 있다. 이러한 문제점을 해결하기 위해 DNS-ALG (DNS-application level gateway)의 기능을 이용하여 목적지 IPv6 주소를 IPv4 호스트가 인식할 수 있는 IPv4 주소로 매핑시킴으로서 IPv4 호스트가 IPv6 호스트에게 패킷을 전송할 수 있다. DNS-ALG는 그림 1과 같이 변환기와 함께 동작하는 애플리케이션 에이전트 기능을 수행한다. DNS-ALG는 DNS query와 response를 통해 IPv4와 IPv6의 주소 전달시 각 네트워크에서 운용되는 IP 주소를 상대 네트워크에서 인식할 수 있는 주소로 변환하는 기능을 수행한다[4~6].

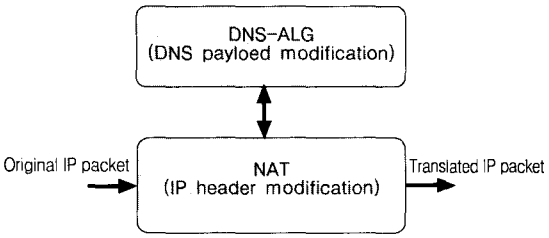

그림 1 NAT와 DNS-ALG의 기능

표 1 IP 버전별 DNS 레코드 형식

Mapping	IPv4	IPv6
Record type	cpe.gwu.ac.kr IN A 128.134.56.134	cpe.gwu.ac.kr IN AAAA 4321:0:1:2:3:4:567:89ab
Domain name	161.56.134.128.IN ADDR.ARPA	b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0. 1.2.3.4.IP6.INT

DNS에서 사용되는 RR와 도메인 네임은 표 1과 같이 각 IP 버전에 따라 다른 형식을 가지고 있다. IPv4의 A 레코드와 IPv6의 AAAA 또는 A6레코드는 이름을 주소로 매핑(name to-address)시키는데 사용된다. 그리고 IPv6.INT와 IN-ADDR.ARPA는 각각 IPv6와 IPv4 도메인 이름으로서 주소를 이름으로 매핑(address-to- name)시키는데 사용된다. DNS-ALG에서는 DNS query와 response 메시지의 RR을 상대 DNS 서버가 인식할 수 있도록 변환하는 과정을 수행하게 되고 이러한 과정에서 실제 주소변환이 이루어지게 된다[4, 5].

그림 2는 인바운드 세션 설정시 변환기와 DNS ALG의 세부동작을 설명하고 있다. 호스트 B의 name resolver는 통신하고자 하는 호스트 A에 대해 name lookup request 데이타그램을 전송한다. 이 데이타그램은 IPv4와 IPv6 사이의 경계라우터에 위치하는 DNS-ALG에 전달된다. DNS-ALG에서는 IPv6 도메인에서 운영될 수 있도록 A 레코드를 AAAA 또는 A6 레코드로 변환하고 IPv4 소스 주소를 128비트의 IPv6 주소로 변환한다. IPv6 DNS 서버에 의해 해결된 IPv6 주소는 IPv4 호스트가 사용할 수 있는 IPv4 주소로 변환되어야 한다. 이를 위해 내부적으로 NAT-PT 변환기에 의해 사전에 유지하고 있는 임시 IPv4 주소 중 하나를 할당한다. DNS ALG를 통한 name resolution의 DNS reply는 표 2와 같이 각 네트워크에서 운영되는 버전에 맞도록 변형된다[4].

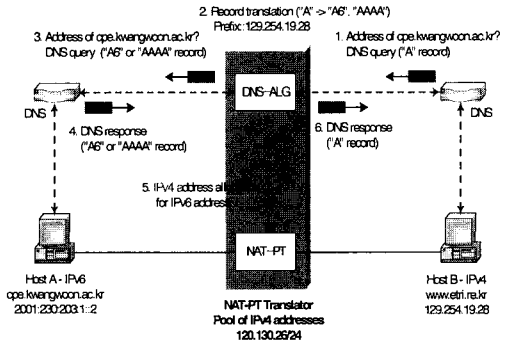

그림 2 인바운드 세션 주소변환

표 2 DNS Reply 변환

Query에 대한 응답	호스트	RR	주 소
DNSv6의 응답	A	AAAA	2001:230:203:1::2
DNS-ALG의 응답	A	A	120.130.26.1

아웃바운드 세션의 주소변환은 인바운드 세션의 주소변환과 달리 목적지 DNS query 메시지 전송시 IPv6 호스트의 IPv6 주소에 임시 IPv4 주소가 할당된다. 그리고 DNS response 메시지 수신시 IPv4 호스트의 주소에 prefix를 추가하여 IPv6 주소로 변형하여 사용한다. 아웃바운드 세션에서는 주소 변환 외에 포트 변환을 사용하여 임시 IPv4 주소를 효과적으로 운용할 수 있다. 포트 변환은 IPv6 노드의 TCP/UDP 포트를 할당된 IPv4 주소의 63K TCP/UDP 포트중의 하나로 변환한다. 따라서 IPv6 호스트가 하나의 임시 IPv4 주소를 사용하는 IPv4 호스트와 투명하게 통신할 수 있다. 결국 변환에 사용되는 임시 IPv4 주소들이 고갈되면 새로운 IPv6 호스트가 IPv6 네트워크 외부의 IPv4 호스트와 세션을 설정할 수 없는 NAT-PT의 단점을 극복할 수 있다. 그러나 NAPT-PT는 아웃바운드 세션에만 적용될 수 있고, 인바운드 세션에서는 목적지 호스트들에 대한 식별 문제 때문에 적용될 수 없는 단점이 있다[3].

3. IPv4/IPv6 프로토콜 변환

IPv4와 IPv6는 버전별 프로토콜의 기능이 조금씩 다르고 각 기능을 담당하는 헤더의 형식이 다르다. 따라서 다른 버전의 IP를 사용하는 호스트들의 경우 상대 호스트의 프로토콜을 이해할 수 있도록 주소변환과 함께 이러한 패킷들의 헤더 변환기능이 추가되어야 한다. 헤더 변환이 필요한 프로토콜은 크게 IP와 ICMP로 구분할 수 있다. 표 3은 인바운드 세션의 기본 헤더 변환시 분할(fragmentation)의 유무에 따른 각 필드들의 변환방법을 설명하고 있다. 표 3에서와 같이 분할에 관련된 정보가 IPv4에서는 기본 헤더에서 표현되지만 IPv6에서는 next header에서 표현된다. IPv6의 Payload length 필드, IPv4의 Header length 필드와 Total length 필드간의 변환 시에는 fragment header의 존재 여부를 고려하여 각 필드 값이 재 계산되어야 한다[4, 6].

ICMPv6, TCP, UDP의 Checksum 필드는 표 4와 같이 계산의 범위가 헤더 외에 데이타나 메시지 필드까지 포함하고 있기 때문에 16비트 연산을 위한 패딩을 위해 가상 헤더(Pseudo Header)를 필요로 한다. TCP나 UDP의 가상 헤더가 데이타그램 전달의 신뢰성을 위해 IP 주소정보를 이용하므로 주소정보를 이용하는 호스트들을 위해 가상헤더의 checksum도 재 계산되어야 한다[4, 6].

IPv6에서는 path MTU(Maximum Transfer Unit) discovery가 항상 수행되지만 IPv4에서는 선택적으로 동작된다. 또한 MTU 초과에 따른 패킷 분할기능 수행

표 3 분할(Fragmentation) 유무에 따른 인바운드 세션의 헤더변환

IPv6 field	Translation without fragmentation	Translation with fragmentation
Version	6	6
Traffic Class	• Copied from IP TOS if identical • Ignore the IPv4 TOS, set 0	좌동
Flow label	• All bit zero	좌동
Payload Length	• Total length of IPv4 header (IPv4 header + IPv4 options)	• (Total length of IPv4 + fragment header) - (IPv4 header + IPv4 options)
Next Header	• Copied from IPv4 header	• Fragment header (44) • Fragment header field 복사
Hop Limit	• TTL value of IPv4 since translator is a router	좌동
Source Address	• Low-order 32 bits : IPv4 source address • High order 96 bits:모든 IPv4 통신을 위한 PREFIX PREFIX를 가지는 모든 주소들은 NAT-PT를 경유	좌동
Destination Address	• NAT PT는 destination 노드에 대한 IPv4와 IPv6 주소매핑 유지 • IPv4 destination 주소를 IPv6 주소로 변환	좌동

표 4 프로토콜의 Checksum 영역

Protocol	IPv4	IPv6
IP Checksum	Header	Not applicable
ICMP Checksum	Header + Data	Header + Message
TCP/UDP Checksum	Header + Data	Header + Data

이 IPv6 네트워크에서는 송신측 호스트만이 이 기능을 수행한다. 그리고 IPv6 link는 1,280바이트 이상의 official MTU를 가지는 반면에 IPv4에서는 68바이트를 가진다. 따라서 IPv6-to-IPv4 변환기가 포함된 경로에서의 종단간 path MTU discovery를 하기 위해서는 특별한 방법이 필요하다.

인바운드 세션에서의 path MTU discovery는 IPv4가 path MTU discovery 수행 여부에 따라 두 가지 방법으로 구분된다. IPv4 호스트가 path MTU discovery를 수행하는 경우 그림 3과 같이 IPv4 또는 IPv6 라우터는 송신측에 ICMP packet too big 에러 메시지를 보낼 수 있다. 따라서 이러한 메시지가 IPv6 라우터에 의해 전송된 경우에는 변환기가 이것을 IPv4 노드가 알 수 있도록 변환해 주어야 한다[4]. IPv6 분할 헤더는 IPv4 패킷이 이미 분할되었을 경우에만 포함된다. IPv4 호스트가 path MTU discovery를 수행하지 않는 경우 변환기는 전송되어온 IPv4 패킷이 IPv6 측의 path MTU를 초과하는지를 확인해야 한다. 이 때 IPv6 측에서의 분할을 미리 막기 위한 방법은 IPv4 패킷을 사전에 IPv6 offcial MTU인 1,280바이트를 초과하지 않도록 억제하는 방법과 전송되어온 패킷이 1,280바이트를 초과하는 경우 변환기가 패킷을 분할하고 이 분할정보를 IPv6 확장헤더에 포함하는 방법이 있다[5, 6].

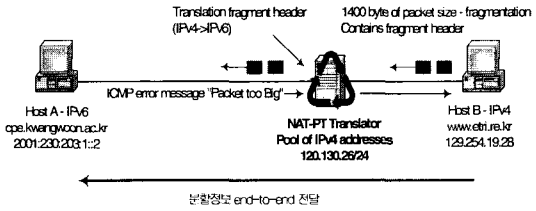

그림 3 IPv4 호스트의 Path MTU discovery

Path MTU discovery 수행시 각 버전별 ICMP 에러 메시지를 변환하고 ICMP 가상헤더의 checksum을 추가하기 위한 별도의 프로토콜 변환 과정이 필요하다. 이 때 변환될 ICMP 메시지들은 ICMPv6가 ICMPv4와 달리 TCP나 UDP처럼 pseudo-header checksum을 가지기 때문에 ICMP Checksum 필드는 재 계산되어야 한다. 추가로 모든 ICMP 패킷들은 각 버전에 적합한 필드 값 변환 과정과 ICMP 에러 메시지 변환 과정이 필요하게 된다. 인바운드 세션에서의 각 ICMP 메시지별 변환은 표 5와 같다[3, 10].

이러한 프로토콜 변환 외에 IP주소 정보를 이용하는 애플리케이션 프로그램의 변환도 고려하여야 한다. FTP의 경우 IPv4 호스트는 FTP 구현을 위해 EPRT와 EPSV command extensions를 사용하거나 사용하지 않을 수도

표 5 인바운드 세션의 ICMP 메시지 변환

Message	Code field	Translation
Destination (Type 3)	Code 0, 1 (net, host unreachable)	Set code to 0 (no route to destination)
	Code 2 (protocol unreachable)	ICMPv6 parameter problem (Type4, Code1) Make the pointer point to the IPv6 next header
	Code 3 (port unreachable)	Set code to 4 (port unreachable)
	Code 4 (Fragmentation need)	ICMPv6 Packet Too Big message with code 0 IPv4와 IPv6 헤더 차이를 위한 MTU field 필요
	Code 5 (source route failed)	Set code to 0 (no route to destination)
	Code 6, 7, 8	Set code to 0 (no route to destination)
	Code 9, 10	Set code to 1 (communication with destination administratively prohibited)
	Code 11, 12	Set code to 0 (no route to destination)
Redirect (Type 5)		Single hop message, silently drop
Source Quench (Type 4)		Obsoleted in ICMPv6, silently drop
Time Exceeded (Type 11)		Set the type field to 3 (code field is unchanged)
Parameter Problem (Type 12)		Set the type field to 4 (pointer 필요)

있다. 만일 FTP 세션을 생성한 IPv4 호스트가 PORT 또는 PASV command를 사용한다면 FTP-ALG는 이러한 명령어들을 IPv6 호스트에 전달하기 위해 EPRT와 EPSV 명령어로 변환해야 한다. 반대로 IPv4 호스트가 EPRT와 EPSV command를 사용하여 FTP세션을 생성한다면 FTP-ALG는 command 자체를 고치지 않고 단지 이러한 command의 파라미터만을 변환하면 된다. 즉, number <net-prt> 필드는 AF #1에서 AF #2로 변환되고 <net-addr>는 ASCII 형식의 IPv4주소에서 string-notation 형식의 IPv6 주소가 할당된 NAT PT로 변환된다. 그리고 EPSV response의 <tcp-port>변수는 NAPT-PT의 경우에만 변환된다[4, 6].

4. NAT-PT 기반의 IPv4/IPv6 변환기 설계

4.1 변환기의 프로토콜 계층

본 장에서는 NAT-PT 표준을 기반으로 포트 변환 방식을 응용한 좀 더 효율적인 NAT-PT 변환기 모델에 대해 고찰한다. 제시한 모델은 양방향 세션의 NAT PT 방식과 임시 IPv4 주소를 효율적으로 운영할 수 있도록 하는 아웃바운드 세션의 포트변환 방식의 혼용이 특징이다. NAT-PT 변환기는 IP 계층과 데이타 링크 계층 사이에 NAT-PT 모듈이 위치하도록 하였다. 이를 위해 IPv4 네트워크와 IPv6 네트워크로부터 수신되는 패킷에 대해서 그림 4와 같은 구성을 통해 상위 계층에서부터 하위계층으로 처리하도록 하여 상위 계층의 필드 변경이 하위 필드에 모두 반영되도록 하였다[5, 10].

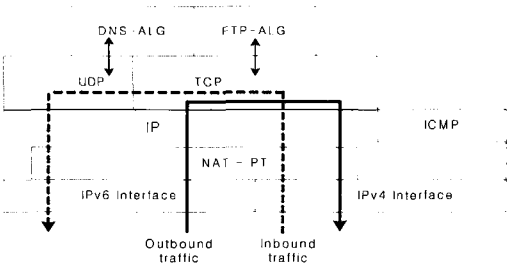

그림 4 NAT-PT 변환기 프로토콜 계층 및 패킷 플로우

각 버전별 인터페이스를 통해 NAT-PT 변환기에 패킷이 수신되면 NAT-PT 모듈은 그림 5와 같이 IP 헤더의 Version 필드의 IP 버전을 확인하여 이 패킷이 변환을 필요로 하는지를 판단한다. 그리고 NAT-PT는 패킷 필터링을 통해 목적지 주소를 검사하여 각 버전별 패킷의 변환처리 또는 native 프로세싱 여부를 결정한다. IPv6 호스트로부터 전송된 패킷의 목적지 주소가 IPv6 호스트인 경우에는 목적지 주소 형식이 콜론(:)을 사용하여 8개의 16비트 단위로 구분되어 구성된다. 패킷의 목적지 주소가 IPv4 호스트인 경우에는 목적지 주소 형식이 96비트의 prefix를 사용하여 prefix::w.x.y.z의 형식을 가지게 된다. 이러한 주소 형식의 차이점을 비교하면 변환처리를 필요로 하는지 또는 native 프로세싱 여부를 결정할 수 있다.

IPv4 호스트로부터 전송된 패킷의 목적지 주소는 32비트의 형식을 취하고 있기 때문에 목적지가 IPv6 호스

트인 경우 변환이 필요한 패킷일지라도 pool of address로부터 임시로 할당받은 주소를 목적지 주소로 사용한다. 이 경우에는 목적지 주소 형식을 비교할 수가 없기 때문에 인바운드 세션에서 패킷의 변환처리 혹은 native 프로세싱 여부 판단은 별도의 방법이 필요하다. 이를 위해 인바운드 세션에서는 pool of address를 참조하여 만약 목적지 주소가 pool of address의 일부 주소라고 판단되면 실제 목적지가 IPv6 주소를 사용하고 있기 때문에 이 패킷은 변환 처리한다.

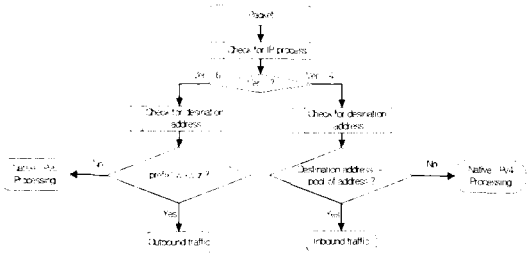

그림 5 패킷 분류를 위한 패킷 필터링 플로우

4.2 인바운드 트래픽 처리과정

변환을 필요로 하는 인바운드 트래픽의 패킷 실제 변환을 위해 그림 6과 같이 NAT-PT 모듈은 우선 IP 헤더의 Protocol 필드를 검사하여 TCP, UDP 또는 ICMP 인지를 확인한다. 상위 프로토콜을 확인한 후 TCP의 경우에는 포트 넘버 등이 매핑 테이블에 존재하는지를 확인하여 세션의 initialization을 판단한다. 만일 세션이 존재하는 경우에는 pseudo checksum을 재계산한 후 IP 계층에서 미리 정의된 변환방법에 따라 IP헤더의 각 필드별 프로토콜 변환을 수행한다. 그리고 매핑테이블 정보를 이용하여 IPv4 주소를 IPv6 주소로 변경한 후 매핑 테이블의 타이머를 갱신하고 나서 최종적으로 IPv6 데이타그램으로 변환된다.

타이머 초과 후의 재전송과 같은 세션 initialization인 경우에는 매핑 테이블에 새로운 세션에 대한 매핑 정보를 기록할 수 있는지에 대한 판단이 필요하다. 만일 가용하지 않은 경우에는 패킷을 버리고 반대의 경우 새로 세션을 설정한 후 이 세션에 대한 매핑정보를 기록 유지하게 된다. ICMP 메시지는 크게 오류보고(error-reporting) 메시지와 query 메시지로 구분될 수 있다. 오류 보고 메시지는 라우터나 호스트가 IP 패킷을 처리하는 도중 발견되는 문제를 보고하는데 사용된다. 그리고 query 메시지는 호스트나 네트워크 관리자가 라우터나 다른 호스트로부터 특정 정보를 획득하기 위해 사용된다. 따라서 ICMP의 세션 구분을 위해 query 메시지는 ICMP 헤더의 Identifier와 Sequence number 필드를 사용한다. 즉, Identifier 필드는 문제 그룹을 정의하고 Sequence number 필드는 특정 echo request와 같은 메시지를 추적할 수 있기 때문에 Identifier 필드를 분석하여 세션 initialization인지를 판단할 수 있다.

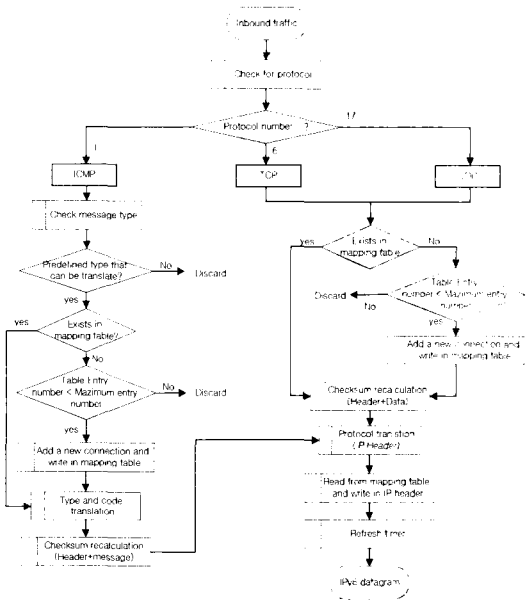

그림 6 인바운드 세션의 변환 플로우

4.3 아웃바운드 트래픽 처리과정 및 개선사항

아웃바운드 세션의 변환방법은 그림 7과 같이 인바운드 세션 경우와 거의 동일하다. 다른점은 인바운드 트래픽에서는 목적지 IPv6주소와 IPv4 pool of address로부터 할당된 IPv4간의 매핑방식인 반면에 아웃바운드의 경우에는 IPv6 호스트들에 대한 하나의 대표 IPv4 주소를 사용한다. 그리고 호스트들의 구별을 위해 포트 변환 방식의 source port 매핑방식을 사용한다. 인바운드 세션에서는 DNS-ALG를 통해 DNS response의 IP 주소가 변환될 때 IPv4 pool of address로부터 하나의 주소를 임시로 할당받은 후 이러한 매핑정보가 NAT-PT 매핑 테이블에서 유지된다. 그러나 아웃바운드 세션의 경우에는 IPv4 목적지 주소에 prefix를 덧붙여서 목적지 주소로 사용한다. IPv6 호스트 자신의 주소를 위해 실제 패킷 전송단계에서는 이 주소에 매핑될 IPv4 주소 혹은 포트를 할당받게 된다. 이러한 모델의 장점은 IPv4 pool of address의 효율적인 사용에 있다. 설계된 NAT

-PT 변환기는 포트 변환 방식과 유사하게 IPv6 호스트들을 대표할 IPv4 주소를 여러 개 두고 63K의 port를 운영함으로써 적은 IPv4 주소로 효율적인 임시 주소 운영을 할 수 있다.

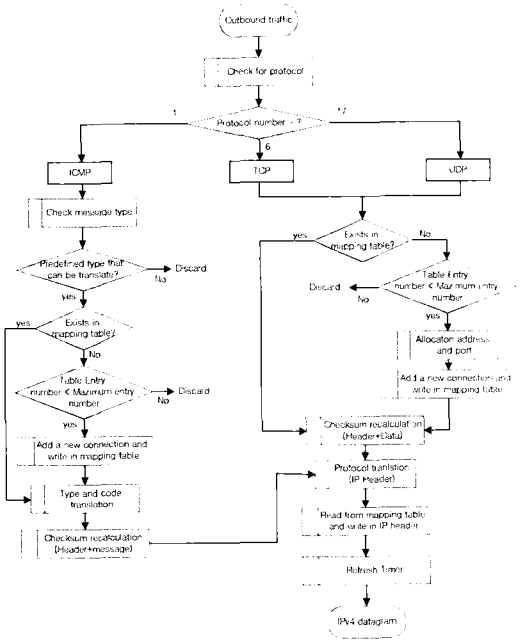

그림 7 아웃바운드 세션의 변환 플로우

4.4 애플리케이션 처리과정

주소변환과 헤더 변환과정 외에 고려해야 할 또 하나의 기능은 실제 변환시 애플리케이션 레벨에서 동작하는 DNS-ALG와 FTP-ALG의 구현이다. 세부적으로 DNS는 UDP 혹은 TCP를 사용하는데 어느 경우이던 DNS 서버에 의해 사용되는 well-known 포트는 53이다. DNS 응답 메시지가 512바이트보다 작으면 UDP를 사용하는데 이는 최대 UDP 패키지의 크기가 512바이트로 제한되기 때문이다. 반대로 응답 메시지의 크기가 512바이트 이상이면 TCP 연결이 사용된다. 그림 8에서의 DNS-ALG의 플로우 차트는 인바운드 세션과 아웃바운드 세션의 구분 없이 address-to-name과 name-to-address의 query 메시지와 response 메시지를 처리하는 방법에 대해 설명하고 있다. 구현시에는 그림 8과 같이 트래픽의 종류를 구분하여 인바운드 세션의 경우에는 DNS-ALG의 response 메시지 처리과정에서 IPv6 호스트의 IPv6 주소 대신에 IPv4 pool of address의 한 주소를 할당한다.

FTP-ALG의 경우 NAT PT에서는 그림 8에서와 같이 FTP 서비스에서 데이타 전송을 필요로 하는 PORT, PASV, EPRT, EPSV command가 포함된 패킷을 수신하게 되었을 때 command의 버전별 변환이나 파라미터만을 변환하게 된다. 그리고 TELNET 서비스는 TCP만을 사용하여 하나의 채널로 제어정보와 데이타 정보전송이 이루어진다. 따라서 NAT-PT는 하나의 연결정보만을 매핑테이블에 저장하여 기본적인 변환수행을 할 수 있다. PING 서비스는 네트워크 계층없이 IP 계층에 ICMP type 8 (Echo)과 0 (Reply)를 이용하여 제공되기 때문에 각 연결을 구분하기 위한 포트번호가 필요없이 각 연결마다 생성되는 다른 값을 갖는 Identifier 필드를 이용하여 각 연결을 구별할 수 있다.

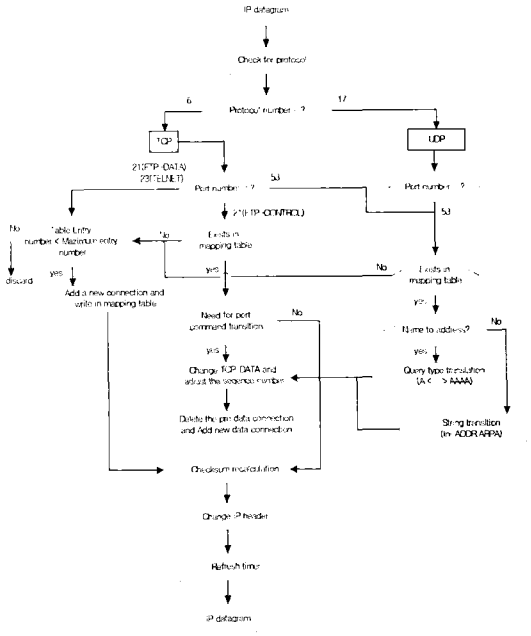

그림 8 애플리케이션 변환 플로우

4.5 매핑 테이블

세션 설정후 일정기간 동안 패킷을 전송하는 경우에는 새로운 주소를 할당받거나 또는 별도의 변환없이 세션 설정시 작성된 매핑 테이블의 매핑정보를 이용하여 패킷을 변환한다. 세션 설정시 작성되거나 일정기간 유지되는 매핑 테이블은 표 6과 같다. 매핑 테이블에서 sequence delta를 사용하는 이유는 TCP가 신뢰성 있는 연결을 보장하기 위해 사용하는 sequence number 때문이다[10]. Sequence number는 세그먼트에 포함된 데이타의 첫번째 바이트에 부여되는 번호로서 목적지

TCP에게 세그먼트의 첫번째 바이트가 이 sequence number에 해당되는 바이트라는 것을 알려준다. 연결설정 단계동안 각 TCP에서는 난수 발생기를 이용하여 ISN(Initial Sequence Number)을 만들며 이 때 사용되는 ISN은 각 방향에 따라 일반적으로 다른 번호가 사용된다. sequence의 증감 크기가 매핑 테이블의 해당 제어 채널에 저장되어야 한다. 예를 들어, 3ffe:2e01:14::1234:5678 호스트의 주소가 NAT-PT 라우터에서 128.134.56.161로 변환되면 주소값들이 ASCII 코드값으로 표현되기 때문에 전체 데이타의 길이가 감소하게 된다. 따라서 TCP 헤더의 sequence를 변경된 길이만큼 증가시키고 NAT 테이블에 변경된 길이만큼 감소시켜 TCP sequence를 보존할 수 있도록 해야 한다.

타이머는 표 6과 같이 매핑 테이블에 세션에 관계된 매핑 정보들이 유지되는 시간이다. 기존 NAT에서의 값을 기준으로 TCP의 경우 900초 정도로 설정하고 UDP의 경우에는 180초 정도로 유지한다. 그리고 더 이상의 값이 필요할 경우에는 적합한 값으로 운영할 수 있다. TCP의 경우 세션이 끝나고 다시 바로 세션을 설정할 수도 있기 때문에 TCP 헤더의 Code 필드에 있는 FIN 비트가 설정된 패킷이 수신되더라도 매핑 테이블의 연결 정보를 삭제하지 않고 타이머 값에 따라 운영되도록 한다. UDP 헤더의 경우에는 Code 필드를 가지고 있지 않기 때문에 순수하게 타이머만을 사용하여 매핑 테이블을 유지한다. 그리고 Trans-IPv6 포트는 아웃바운드 세션의 경우에 해당되는 엔트리로서 표 6과 같이 pool of address을 효율적으로 사용하기 위하여 NAT-PT 라우터를 나타내는 IPv4 주소 128.222.32.31이 할당한 후 포트넘버로 IPv6 호스트를 구별하도록 한다. 매핑 테이블의 엔트리는 최대 1,000개 정도로 설정하도록 하는데 운영환경에 따라 값은 변경될 수 있다.

5. 결 론

본 논문에서는 IPv6의 도입에 따른 IPv4와 IPv6간의 트랜지션 메커니즘의 설계에 필요한 요소 기술들을 분석하였다. 분석된 요소기술들은 IPv4/IPv6 주소변환과 IPv4/IPv6 및 ICMPv4/ICMPv6 프로토콜 변환부분으로 크게 구분하였으며 설계에 필요한 기능들을 도출하여 NAT-PT 메커니즘 기반의 효율적인 모델을 제시하였다. 제안된 NAT-PT 변환기 모델은 IPv4 주소를 필요로 하는 모든 호스트에게 IPv4 주소를 할당하는 표준 방식 대신에 단일 임시 IPv4 주소와 포트를 할당하여 호스트를 식별함으로써 할당되는 IPv4 주소를 최소화하였다. 이러한 방식을 사용함으로써 변환기에서 유지할 수 있는 세션의 수가 아웃바운드 세션의 경우 IPv4 주소의 63k배가 되기 때문에 주소 효율성 측면에서 큰 장점을 가진다. 그리고 포트변환의 특성을 이용하여 사설망 또는 초기 IPv6망의 방화벽 기능을 수행할 수 있도록 하였다.

또한 본 논문에서 제안한 NAT-PT 메커니즘은 이미 기능이 검증된 기존 NAT 기능과 유사하게 동작하도록 설계하였다. 그리고 DNS ALG 기능을 추가하여 양방향 세션에 대한 변환기능의 호환성을 제공하였고 표준에서 언급되지 않은 실제 구현과정에서의 매핑 테이블 관리 및 타이머 설정 등 세부 구현 기술에 대해 설명하였다. 제시된 모델의 이러한 특징들은 IPv6 초기 도입 단계에서 소수의 IPv6 호스트가 기존의 IPv4 네트워크와 연동하여 패킷을 전송할 수 있기 때문에 완전한 IPv6 도입 이전까지는 과도기적인 수단으로써 제시될 수 있다.

그러나 아직 구현을 위한 IPv6와 ICMPv6의 각 필드별 기능과 값이 완벽하게 정의되어 있지 않기 때문에 분할과 같은 세부 기능들은 고려하지 않고 기본 변환 기능만을 고려하여 알고리즘을 설계하였다. 향후 세부적인 필드값들을 정의함으로써 이러한 제한들이 해소될 수 있고 좀 더 효율적인 알고리즘의 개선이 이루어질 수 있다. 그러나 NAT-PT는 기본적인 기능의 구현으로도 향후 이동통신망의 이종 통신망과의 연동이나 mobile IP에서 MIPv4(Mobile IPv4)와 MIPv6(Mobile IPv6)의 연동에 사용될 수 있으며 통신사업자의 소규모 IPv6 서비스에도 적용될 수 있다.

표 6 매핑 테이블

Num	IPv4 address	IPv4 port	IPv6 address	IPv6 port	Trans IPv6 port	Sequence delta	Timer (sec)	Protocol
1	128.134.56.161	2048	2001:230:203:1::3	21	21	21	900	TCP
2	128.156.123.52	1635	2001:230:203:1::7	53	53	0	180	UDP
3	128.222.32.31	21	2001:230:203:1::5	654	1456	20	180	UDP
4	128.222.32.31	267	2001:230:203:1::13	2789	1457	20	900	TCP

참 고 문 헌

[1] S. Deering *et al.*, "Internet Protocol, Version 6 (IPv6) specification," IETF RFC 2460, December 1998.

[2] 이승민, 민상원, 이숙영, 신명기, 김용진, "IPv6망에서 DSTM을 이용한 IPv4 서비스 제공 방안", 정보과학회 추계학술대회, 2001년 10월.

[3] W. Stallings, "IPv6: the New Internet Protocol," *IEEE Communication Magazine*, Vol. 34, No. 7, July 1996.

[4] G. Tsirtsis *et al.*, "Network Address Translation Protocol Translation (NAT-PT)," IETF RFC 2766, February 2000.

[5] 이승민, 민상원, 김용진, 박수홍, "IPv4 와 IPv6의 연동과 호환을 위한 NAT-PT에 관한 연구", 정보과학회 추계학술대회, 2000년 10월.

[6] P. Srisuresh *et al.*, "DNS extensions to Network Address Translators (DNS_ALG)," IETF RFC 2694, September 1999.

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

[8] H. Hui and M. Jian, "IPv6-future approval networking," *WCC-ICCT 2000 Communication Technology Proceedings*, Vol. 2, pp. 1734-1739, 2000.

[9] H. Afifi and L. Toutain, "Methods for IPv4 IPv6 transition," *IEEE computers and Communications Proceedings*, pp. 478-484, 1999.

[10] 고문준, 민상원, "TCP/IP 주소 변환기능 구현", 한국정보과학회 논문지 제 28 권 제 1 호, 2001년 3월.

[11] S. Thomson *et al.*, "DNS Extensions to s upport IP version 6," IETF RFC 1886, December 1995.

[12] J. McCann *et al.*, "Path MTU Discovery for IP version 6," IETF RFC 1981, August 1996.

[13] A. Conta *et al.*, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Verstion 6 (IPv6) Specification," IETF RFC 2463, December 1998.

[14] K. Egevang *et al.*, "The IP Network Address Translator (NAT)," IETF RFC 1631, May 1994.

이 승 민

2000년 2월 광운대학교 전자통신공학과 학사. 2002년 2월 광운대학교 전자통신공학과 석사. 2002년~현재 삼성전자 TN총괄 무선사업부 개발 2그룹. 관심분야는 IPv6, Mobile IP, Wireless Network VoIP, NGN

진 재 경

2001년 2월 광운대학교 전자공학부 학사 2003년 2월 광운대학교 전자통신공학과 석사. 2003년 1월~현재 모다정보통신. 관심분야는 IPv6 Mobile IP, 이동통신망, Linux

민 상 원

1988년 2월 광운대학교 전자통신공학과 학사. 1990년 2월 한국과학기술원 전기 및 전자공학과 석사. 1996년 2월 한국과학기술원 전기 및 전자공학과 박사. 1990~1999년 3월 LG 정보통신 연구원. 1999년 3월~현재 광운대학교 전자공학부 조교수 관심분야는 유무선 통신망, IPv6, NGN 등