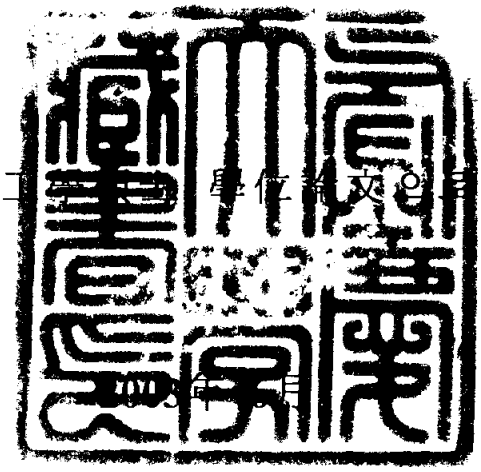
工學碩士 學位論文

IPv6 네트워크에서 Zero Configuration에 기초한 Multicast Address Allocation Protocol 연구

指導敎授 金 成 筧



이 論文을 工學碩士 學位論文으로 提出함

釜慶大學校 産業大學院

情報通信工學科

安 東 燮

安 東燮의 工學碩士 學位論文을 認准함

2003年 6月21日

主　　審　工學博士 河 德 鎬 

委　　員　工學博士 張 珠 錫 

委　　員　工學博士 金 成 篔 

A Study on Multicast Address Allocation Protocol based on Zero Configuration in the IPv6 Networks

Dong-Surp An
Department of Telematics Engineering
Graduate School of Industry,
Pukyong National University

Abstract

With the explosive growth of the Internet and the change of user requirement, current Internet is faced with many problem, such as a growing shortage of address, limitations of speed and multimedia service provision, and security. To solve these problem, IETF(Internet Engineering Task Force) designed the IPv6 protocol as the next Internet protocol.

In this thesis, we initially analyze IPv6 protocol and Zero-configuration mechanism, and then apply them to IP multicast service as an important enabling service for current and future Internet. Throughout this work, we suggest an efficient multicast address allocation method to enable Internet networking without any particular extra configuration and administration.

목 차

그 림 목 차

표 목 차

1. 서 론

범세계적으로 연결되어 있는 TCP/IP 프로토콜은 초기의 연구 망에서 현재 누구나 자유롭게 활용할 수 있는 표준 통신망 프로토콜로 자리잡았다. 해마다 인터넷 사용자 용량은 폭발적으로 증가하여, 향후 2010년경에는 심각한 주소 부족 문제에 직면하게 될 것으로 예상된다. 이러한 문제점을 극복하기 위한 방안으로 IETF (Internet Engineering Task Force)에서는 Ipng WG(IP next generation Working Group)의 승인을 받아 기존의 IPv4에서 발전된 새로운 버전의 Internet 프로토콜로 IPv6 (Internet Protocol version 6)를 제안하였다.

IPv6 프로토콜은 새로운 Internet 주소 체계를 가지며, QoS(Qulity of Service) 보장 및 Multicasting과 Security 기술 등을 지원하는 차세대 Internet 프로토콜로 크게 부각되고 있다. IPv6에서는 기존의 IPv4에서 지원했던 32비트 주소 크기를 128비트로 4배 증가시켰고, 또한 선택 사항들을 제외한 모든 필드들이 고정된 오프셋(Offset)에서 고정된 옥텟 수 만큼을 차지하는 고정 양식 데이터그램 헤더를 사용하는 IPv4와는 달리 선택적인 헤더를 사용하여 IPv4에서 없는 부가적인 기능들을 제공하는 새로운 선택 사항들을 갖게 되었다. 이와 같은 확장 기능으로 인해 IPv6 프로토콜은 하부 망 하드웨어의 변경과 새로운 응용에 보다 효율적으로 적응할 수 있다[1]. 하지만 이러한 기술적인 향상 앞에서도 일반 사용자들은 컴퓨터의 네트워크 설정에 익숙하지 못하고, 또한 늘어나는 사용자들로 인한 네트워크의 유지 보수가 쉽지 않다. 따라서 인터넷 환경에 효율적으로 대응하기 위해, 언제 어디서나 Internet 접속이 가능할 뿐만 아니라 어느 특정 데이터를 다수의 사용자가 동시에 송수신하기를 원하는 응용 프로그램에 대한 대비가

필요한 실정이다. 그러나 현재의 네트워크 환경은 사용자가 Internet에 접속할 경우 반드시 그 환경에 맞는 네트워크 정보를 새로이 설정해 주어야 하고, 다수의 컴퓨터에 데이터 전송 시 특정 Multicast 그룹을 통하여 데이터를 보내기 때문에 불필요한 인터넷 트래픽을 유발하게 된다.

본 논문에서는 Zero-Configuration 개념을 도입하여 컴퓨터에 별도의 네트워크 설정 작업 없이 Internet에 연결포트만 꽂으면 바로 인터넷에 접속할 수 있는 자동 주소 할당 방안과 이를 이용하여 누구나 쉽게 Multicast를 이용할 수 있는 Multicast 주소 할당 방안을 제시 하고자 한다.

이를 위해, 먼저 2장에서는 IPv6 및 Zero-Configuration Networking 기술을 소개하고, 3장에서는 Zero-Configuration 개념을 도입하여 IPv6 기반 네트워크 환경에서 주소 자동 설정 방식을 제안한다. 4장에서는 3장의 연구 방안인 자동 주소 설정 방식을 적용하여 Multicast 상황에서의 자동 주소 할당 방안과 주소 할당 과정에서 야기될 수 있는 혼잡 상황에 대한 대처 방안을 제시한다. 마지막으로 5장에서 본 연구의 결론을 맺고, 향후 연구 방향에 대해 정리한다.

2. IPv6 및 Zero-Configuration Networking 기술 개요

본 장에서는 인터넷이 비약적으로 성장함에 따라, 심각하게 대두되고 있는 인터넷 주소 고갈 문제를 포함해, 정보보호, Multicast, QoS 등의 문제를 해결하기 위한 대안으로 차세대 인터넷 프로토콜(IPv6) 기술 및 관련 연구 동향을 소개하고, IPv6 기반의 네트워크에서의 IP 네트워킹에 필수적으로 요구되는 설정 및 서비스에 대한 자동화 방안인 Zero-Configuration 기술을 소개한다.

2.1 IPv6 기본 구조

IPv6에서는 128비트 주소 체계를 사용함으로써 IPv4에 비해 전체 기본 헤더의 길이는 두 배로 확장되어 40바이트이지만, 영역 수를 12개에서 8개로 단순화시킴으로써 오히려 기본적인 처리 속도를 개선하였다. IPv6의 헤더 구조는 그림2.1과 같다.

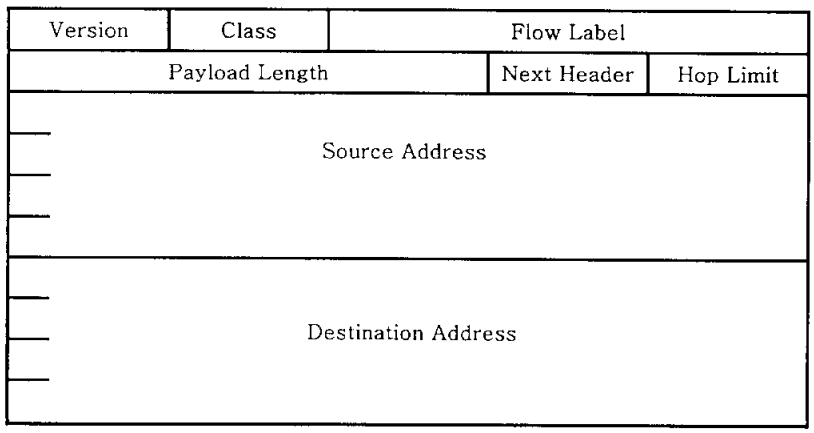


그림2.1 IPv6 헤더 형식

그림2.1에서 "Version" 영역은 인터넷 프로토콜의 버전을 의미하며, 여기서 IPv6를 나타내기 위해 "6"의 값을 가진다. "Class"는 트래픽 등급을 명시해 주는 영역이며, 현재 IETF Diffserv 워킹 그룹에서 이 영역의 활용을 고려하고 있다. 다음으로 IPv4에서는 없었던 "Flow label" 영역은 해당 IPv6 패킷이 속하는 흐름에 대한 특성을 나타내 주며 이 영역에 대한 사용은 아직 표준화되지 않은 상태이다. 이 영역은 QoS 지원을 위해 IP 패킷의 연속적인 흐름을 "플로우"로 정의하고, 이를 식별하기 위한 값으로 사용될 수 있으며, 다른 QoS 관련 그룹의 활동 결과가 추후 반영될 것으로 예상된다. "Payload length" 영역은 IPv6 헤더 다음에 붙는 데이터들의 길이를 표시하며, "Next header" 영역은 IPv6 헤더 다음의 헤더의 종류를 표시한다. 만약 IPv6 헤더의 "Next header" 값이 "0"이면 다음 헤더가 Hop-by-hop 헤더임을 알려준다. 이 영역은 다음에서 기술할 모든 확장 헤더들에도 포함되어, 자신 다음에 위치할 헤더 형식을 명기하기 위해 사용된다. 이처럼 모든 확장 헤더들은 자신을 지칭하는 "Next header" 값을 가지고 있으며, UDP나 TCP 등의 상위 계층 프로토콜들은 IPv4의 프로토콜 영역에서 사용되던 값들을 그대로 사용한다. "Hop limit" 영역은 IPv4에서의 TTL(Time to Live) 영역과 같은 역할을 하며 경유할 수 있는 라우터의 최대 수를 명시한다. 그 이후 나머지 영역들은 각각 128비트의 소스 주소와 목적지 주소 영역으로 구성된다[2]. 또한, 확장 헤더는 패킷 조각화/재조립 또는 소스 라우팅과 같이 IPv4에서 잘 이용되지 않았던 영역이나 옵션들을 위한 것으로 필요할 때에만 사용함으로써 기본 헤더를 간략하게 하여 일반 처리 과정의 효율을 높이게 하였다. 현재 IPv6의 확장헤더는 다음과 같으며, 이와 같은 순서에 따라 사용되어야 한다.

- 홉간 처리 옵션 헤더 (Hop-by-hop Option Header)
- 중간 노드들을 위한 목적지 옵션 헤더 (Destination Option Header)
- 라우터 헤더 (Routing header)
- 조각화 헤더 (Fragmentation Header)
- 인증 헤더 (Authentication Header, AH Header)
- 캡슐화 헤더 (Encapsulating Security Payload, ESP Header)
- 최종 목적지만을 위한 목적지 옵션 헤더 (Destination Options Header)

옵션 헤더는 두 종류가 있는데, 지나가는 홉마다 처리할 옵션을 포함하는 홉간 처리 옵션 헤더(Hop-by-hop Option Header)와 IPv6 헤더의 목적지 주소에 명시되거나 라우팅 목록에 포함된 노드에서만 처리하는 옵션 정보를 포함하는 목적지 옵션 헤더(Destination Option Header)로 구성된다. 라우팅 헤더는 소스 라우팅을 위한 헤더로서 여러 가지 형식을 가질 수 있지만 현재는 중간 라우터 주소들의 목록만 포함하는 가장 간단한 구성의 타입 "0"만 선언되어 있다. 조각화 헤더는 조각화/재조립을 위한 정보를 포함하는 헤더이며, IPv4처럼 중간 노드에서는 이루어지지 않으며 발신지와 목적지 노드에서만 사용될 수 있다. 인증 헤더 및 캡슐화 헤더는 망 계층에서 보안 서비스를 제공하기 위한 헤더이며, 이를 위한 기본 기법 등은 IPsec 그룹에서 표준화를 진행하고 있다.

IPv4에 비해 구별되는 IPv6의 개선 사항은 다음과 같다.

첫째, 라우팅과 주소 지정 기능의 확장이다. IPv6는 IPv4의 32비트 주소영역을 128비트로 확장하였으며, 구조적으로 다양한 형태의 주소를 지정할 수 있다. 즉, "Multicast address" 지원을 통해 Multicast 라우팅의

기능을 보강하였으며, 또한 패킷을 경로상의 노드들 중 하나의 노드에만 전달 시킬 수 있는 “Anycast address" 등과 같이 새로운 유형의 주소가 추가되었다.

둘째, 헤더 형식의 단순화와 융통성을 부여하였다. IPv6에는 기존의 IPv4 헤더 중 일부 영역이 삭제되고 일부는 옵션화하여 기본 헤더를 크게 단순화 시켰다. 그 결과 IP 패킷을 처리할 때 중복적으로 처리되는 부하를 절감 시켰으며, IPv4보다 주소 길이가 4배로 증가하였지만 헤더 전체를 구성하는 세부적인 영역은 감소하였다.

셋째, 옵션기능이 개선되었다. 이는 IP 헤더의 옵션부분의 인코딩 방법을 개선하여 보다 효율적으로 IP 패킷을 전달할 수 있게 하였으며, 또한 새로운 옵션을 융통성 있게 추가하기 위하여 옵션영역의 길이에 대한 제한을 완화하였다.

넷째, QoS (Quality-of-Service) 제어기능을 추가하여 사용자가 요구하는 특정 QoS 수준을 표시할 수 있도록 하였다. 이를 통해, 대역폭과 지연시간에 엄격한 요구사항을 필요로 하는 실시간 서비스 및 멀티미디어 서비스 등을 보다 효율적으로 지원할 수 있다.

마지막으로, 프로토콜 확장이 용이하여 모든 세부 사항들을 전부 지정해 주어야 하는 단점을 개선하여, 부가적인 기능들을 효율적으로 수용할 수 있는 프로토콜로 개선되었다. 이와 같은 확장 기능으로 인해 IETF는 IPv6 프로토콜을 하부 망 하드웨어의 변경 및 새로운 응용에 효율적으로 적용할 수 있는 프로토콜로 규정하였다[3].

2.2 IPv6 주소체계

IPv6에서 할당할 수 있는 주소 공간이 넓어짐에 따라 다양한 주소 할

당 방식을 사용할 수 있으며, 여러 종류의 주소들을 포함할 수 있게 되었다. IPv6 주소에서는 주소의 종류 및 서브넷을 판별할 때 사용하는 64 비트의 Prefix와 네트워크에 연결되어 있는 각 Interface들을 구별해 주는 64비트의 Interface ID로 구성된다. IPv6 망에서 주소를 할당하는 기본 단위는 호스트나 라우터가 아닌 Interface 중심이다. 즉, 같은 호스트에 동일 링크와 연결되는 여러 개의 Interface들이 있을 경우, 각 Interface마다 다른 주소를 할당 받게 된다. 그러나, 일반적으로 한 호스트에 하나의 Interface로 링크에 연결되므로 Interface ID로 호스트를 구분할 수 있게 된다. 또한 기존의 IPv4 주소 체계에서의 사용되던 Unicast 및 Multicast와는 다른 새로운 개념의 Anycast를 도입하였다. 한 라우터가 Anycast 주소를 목적지 주소로 가지는 패킷을 수신했을 경우, 라우팅 프로토콜에 따라 같은 Anycast 주소를 가지는 여러 노드들 중 가장 가까운 노드로만 패킷을 취하는 방식이라 할 수 있다.

IPv6 주소의 표기는 8개의 16진수 4자리 숫자를 콜론(:)으로 구분하여 표기한다. 주소의 길이가 길기 때문에, 0이 연속되어 있는 구간에 대해서는 한번에 한하여 두개의 콜론(::)으로 표시할 수 있게 하였다. 아래의 예에서 처럼, 두 가지 표현 방법은 같은 주소를 의미한다.

201:230:1:0:0:1:2:3

201:230:1::1:2:3

그러나, 위와 같은 표기법만으로는 IPv6 주소를 완벽하게 표현할 수 없다. 앞에서도 언급한 것처럼, IPv6 주소는 각각 64비트로 구성된 Prefix와 Interface ID 영역으로 나눈다. 이 Prefix 영역은 논리적인 계층 구조에 따라 이용되기 때문에 상위 노드에 의해 할당된다고 할 수 있

다. 그러므로, 이 상위 노드의 정책에 따라 다른 길이의 Prefix가 사용되므로, 128비트 주소만으로는 어디까지가 Prefix 영역인 지를 판별할 수 없다. 따라서, Prefix 길이에 대한 정보를 '/' 다음에 10진수로 명시해서, Prefix의 비트단위의 길이를 알 수 있게 하는 것이다. 만약 위의 주소에서 Prefix의 길이가 48비트일 경우 다음과 같이 표시한다.

201:230:1::/48

또한, 웹 브라우저에서 IP주소와 일대일 관계에 있는 FQDN (Fully Qualified Domain Names)을 URL (Uniform Resource Locator)로 표기하는 것 대신에 상대방 IP 주소와 응용 포트(Port)를 직접 명기할 수도 있다. 이 경우, IPv4에서는 포트를 IP 주소와 구분하여 표기하기 위해 콜론(:)을 사용한다. IPv6는 콜론을 이미 다른 용도로 사용하고 있기 때문에, 중괄호([])를 이용해서 이 문제를 해결한다.

예 : http://[201:230:1::1:2:3]:80/pec_ast.html

표2.1 IPv6 주소 할당

주소 할당	Prefix	
Reserved	0000 0000	
Reserved for NSAP	0000 001	
Reserved for IPX	0000 010	
Aggregatable global unicast address	001	2001::/16 2002::/16
Link local unicast address	1111 1110 10	FE80::/10

Site local unicast address	1111 1110 11	FEC0::/10
Multicast address	1111 1111	FF00::/8

표2.1에서 이미 할당되어 있는 IPv6의 각 주소 영역과 이를 식별하는 Prefix 값을 나타냈다.

"0000 0000" Prefix 영역은 특수 목적용 주소 영역으로, 여러 가지 용도로 사용된다. 첫번째는 자신 호스트의 생존여부 등을 확인하기 위해 사용되는 Loopback 주소이며, "::1"로 표기된다. 두번째로 IPv4와의 호환을 위해 사용된다. IPv4 주소를 그대로 IPv6주소 영역에 포함시키기 위해 사용하는 IPv4-compatible (예, ::203.255.255.130) 주소나 IPv6 스택을 갖추지 못한 호스트 상에서의 IPv6 주소를 시스템 내부에서만 유효하게 사용하고자 할 때 사용되는 IPv4-mapped (예, ::ffff:203.255.255.130) 주소 등이 이에 속한다.

두 번째와 세 번째의 예약 영역은 TCP/IP 스택이 아닌 ISO 및 IPX 계열의 프로토콜들을 위해 예약된 곳이다.

Aggregatable global unicast address 영역은 일반적인 IPv6 주소 영역이며, 이 영역에서의 주소는 계층 구조에 따라 할당된다.

Link-local 주소 및 Site-Local 주소는 모두 해당 영역 안에서만 의미를 가지는 주소이다. 이 때 Interface ID로 사용되는 값들은 Link나 Site에서 고유한 값이어야 한다. 따라서 링크 계층 주소들이 이들 Prefix 뒤에 사용될 수 있다.

마지막 영역은 Multicast 주소를 위한 Prefix이다. 나머지 표시하지 않은 영역들은 아직 할당되지 않은 부분들이다[4][5].

2.3 IPv6 관련 연구 동향

가. IETF 표준화 동향

1994년 인터넷 관련 국제표준을 제정하는 IETF IPng WG에서 IPv6 규격을 표준화한데 이어 1996년 IETF NGTrans WG 에서는 6bone(IPv6 Backbone)이란 시험망을 만들어 관련 기술에 대한 시험적 운영과 IPv6로의 전환 기술에 대한 연구를 수행하고 있으며, 1999년에는 6REN(IPv6 Research and Education Network)이란 상업적 단계의 네트워크를 구성하여 본격적인 IPv6의 서비스를 준비하고 있다.

현재 IETF에서는 IPv6 구조, 어드레싱, ICMPv6(Internet Control Message Protocol), NDP(Neighbor Discovery Protocol), MLD (Multicast Listener Discovery), PMTU(Path Maximum Transmission Unit) Discovery, IPv6-over-Ethernet 등 기본 표준 규격에 대한 표준화는 거의 완료한 상태이며, Mobile IPv6, Header compression, DNS & reverse DNS extension, IPv6-over-NBMA 등 추가적인 사항들에 대한 표준화 작업을 진행중이다. IPv6 전환작업과 관련된 표준작업으로는 6bone 규칙 등에 관한 표준이 제정되었고, 현재 IPv4/IPv6 전환 메커니즘에 관해 SOCKS, SIIT(Stateless IP/ICMP Translation), NAT-PT(Network Address Translation-Protocol Translation), BIS (Bump In the Stack), DSTM(Dual Stack Transition Mechanism), 6 to 4, Tunnel Broker 등 다양한 방식에 대해 표준화 작업이 진행중이다[6].

나. IPv6 포럼 동향

IPv6 포럼(IPv6 Forum)은 올해 초 IPv6의 도입 및 관련 시장의 활성화를 위해 전세계적으로 만들어진 컨소시엄으로 회원제로 운영되며 현재

미국의 마이크로소프트, 시스코, 선 마이크로시스템즈, 컴팩, AT&T, 유럽의 Case Technology, Thomson-CSF, 일본의 Hitachi, WIDE 등 전세계 주요한 기업 및 ISP, 연구소 등 80여 개 기관이 회원으로 가입되어 있고, 국내에서도 ETRI와 KT가 회원으로 등록되어 있는 등 앞으로 IPv6 도입의 방향을 결정짓는 주요한 역할을 할 것으로 보인다[7].

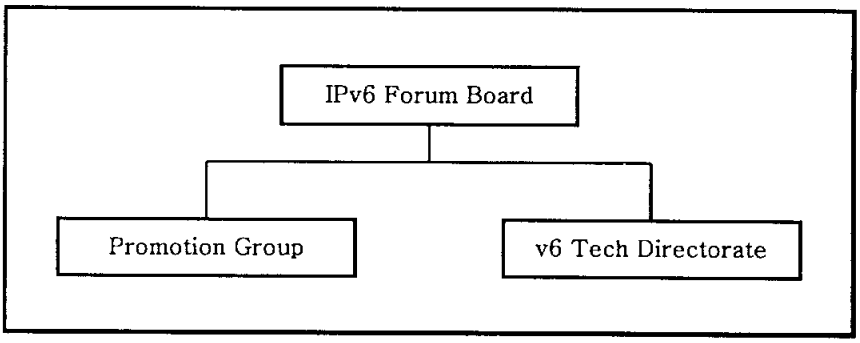


그림2.2 IPv6 포럼 구조

IPv6 포럼은 ISOC 및 IETF IAB, IPng WG에 의해 지원 받고 있으며, 그 구조는 IPv6 Board 아래에 Promotion 그룹과 Deployment 그룹으로 나누어 조직되어 있다. Promotion 그룹은 Education & Aware-ness(EA) WG, Project WG, Global IPv6 Summit, IPv6 Forum Public Relations, Alliance Program, Fellow Program 등으로 조직되어 있으며, 현재 15개의 벤더들이 가입되어 있다. Deployment 그룹은 Technical Directoriate로 구성되며 현재 20명의 전문가로 구성되어 있다(그림2.2 참조).

EA WG과 PR WG은 IPv6의 기술에 대한 홍보 및 교육을 목적으로 웹 사이트 구축, 문서 및 자료 제공, 전환 도구의 홍보 등을 주된 역할로 하고 있다. 현재 IPv6 백서와 같은 기술 가이드 작성을 고려중이며, 문서 작성 시 다중언어(영어, 일본어, 스페인어)의 고려 및 IPv6의 전환을

도움주기 위한 논문 작성 등에 대한 논의가 진행중이다. Project WG은 IPv6 관련한 프로젝트의 후원 및 발굴을 목적으로 하고 있으며, 현재 유럽을 중심으로 하는 다음과 같은 프로젝트들을 후원하고 있다.

- 6INIT: IPv6 Internet Iniative의 약자로 유럽의 Telebit, BT, Thomson-CSF 등 10개 기관에서 80여 명이 참가하고 있는 유럽의 IPv6 도입을 위한 프로젝트
- AMX-IX: 독일의 native IP 망 구축 프로젝트
- SILK-LOAD NG: EU와 일본의 공동 프로젝트

IPv6 Forum Public Relations, Alliance Program, Fellow Program 등에서는 IPv6 기술을 필요로 하는 다른 기관과의 협력을 목표로 하고 있으며, 현재 UMTS Forum, GSM Association, QoS Forum, GIP Forum, ETSI, EU 등과 협력방안을 논의하고 있다.

마지막으로 Technical Directoriate는 IPv6 도입을 위한 기술적인 부분을 책임지고 있고, IPv6 기술의 20여 명의 전문가들이 위촉되어 있으며, 포럼의 방향을 결정짓는 역할을 하고 있다. Technical Directoriate는 현재 Jim Bound와 Perry E. Metzger가 공동의장을 맡고 있다. 현재 technical white paper 작성, UMTS, W3C 등에 liaison 전송 및 관련 다른 기구와의 관계 등에 대한 논의를 진행중이다.

2.4 확장된 ICMPv6(Internet Control Message Protocol version 6)

인터넷은 전송 방식의 특성상 전송된 패킷에 대해 완벽하게 신뢰성을 제공할 수 없기 때문에, 에러 상황의 보고와 정보 메시지의

전달을 위한 제어 메시지 교환 절차가 필요하며, 이러한 기능을 ICMP 프로토콜이 수행한다. 기존의 IPv4에서와 같이 IPv6도 동일한 목적을 위해 이러한 제어 프로토콜이 필요하며, 기존의 ICMP를 확장한 ICMPv6를 사용한다. 즉, ICMPv6는 IPv6 노드에서 패킷 처리 시 발생한 에러를 진단 및 보고하는 기능을 수행하며, IPv6를 구현하는 노드들은 반드시 ICMPv6의 완벽한 구현이 요구된다.

본 논문의 3장에서는 이러한 ICMP 패킷을 이용하여 자동 주소 설정 시 주소 중복 검사를 위해 사용한다.

그림2.3은 ICMPv4에서 확장된 ICMPv6의 기능 블럭을 나타낸다.

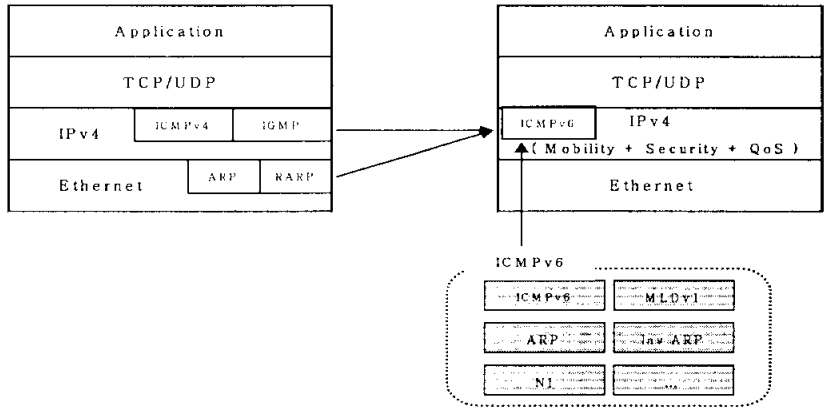


그림2.3 ICMPv4와 ICMPv6 비교

기존의 ICMPv4처럼 ICMPv6도 크게 두 가지 카테고리, 즉, 에러 메시지와 정보 메시지의 두 부류로 나눌 수 있는데, 에러 메시지는 메시지 유형 영역 값의 상위 비트가 "0"인 것으로 식별할 수 있다. 에러 메시지 유형은 "0"에서 "127"사이의 정수 값을 가지며, 정보 메시지는 "128"에서 "255" 사이의 값으로 식별된다. 표2.2는 현재까지 정의 되어있는 메시지 유형들을 나타내며, IPv6 기본헤더와 IPv6 확장헤더에 이어서 나타나는 ICMPv6 메시지의 일반적인 형식은

그림2.4와 같다.

표2.2 ICMPv6 메시지 유형

Error Messages	1	Destination Unreachable Error
	2	Packet Too Big Error
	3	Time Exceeded Error
	4	Parameter Problem Error
Information Messages	128	Echo Request
	129	Echo Reply
Group Membership Messages	130	Group Membership Query
	131	Group Membership Report
	132	Group Membership Termination
Router Discovery Messages	133	Router Solicitation
	134	Router Advertisement
Neighbor Discovery Messages	135	Neighbor Solicitation
	136	Neighbor Advertisement
Redirection Message	137	Redirect

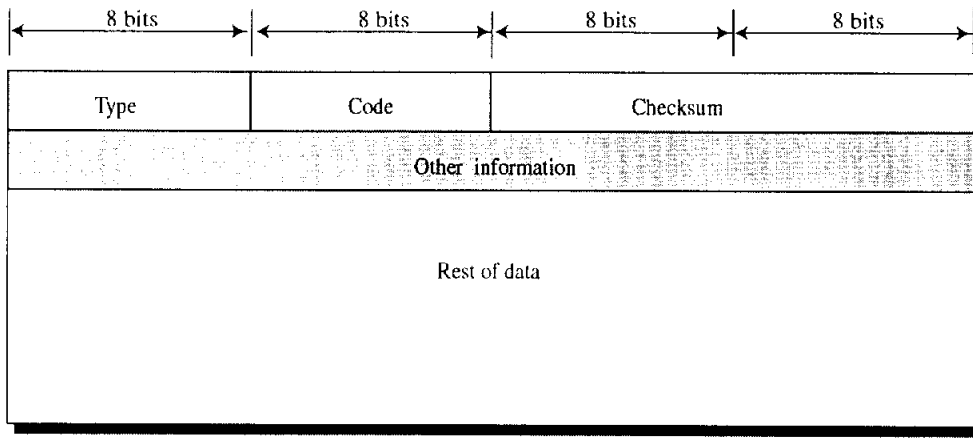


그림2.4 일반적인 ICMPv6 메시지 형식

ICMPv6 메시지 형식에서 "Type" 필드는 메시지 유형을 나타내며, 그 값에 따라 나머지 데이터의 형식을 판별할 수 있다. "Type" 필드 다음의 "Code" 필드는 메시지 유형에 따라 추가적으로 상세하게 메시지를 분류하기 위해 사용된다. "Checksum" 필드는 ICMPv6 메시지 및 IPv6 헤더 부분의 에러를 찾아내기 위해 사용되며, "data"는 메시지의 유형에 따라 서로 다른 구조를 가진다[9][10].

표2.2에 나타난 것과 같이 ICMPv6에는 6개의 메시지 형태를 지원한다.

본 논문에서는 "Type" 필드의 133 ~ 138까지의 형태 메시지를 사용하여, 인접노드의 정보를 획득하고, 자동 주소 설정 시 주소 중복 검사를 실시하기 위해 사용한다. 먼저 인접 탐색 프로토콜(Neighbor Discovery)은 ICMPv6의 정보 메시지들을 이용하여 동일 링크에 연결된 이웃 노드 간의 상호 동작에 관련된 다음과 같은 일련의 기능들을 수행하기 위해 사용된다.

첫째, 호스트가 연결한 링크에 상주하는 라우터의 위치를 찾는다.

둘째, 노드가 목적지 노드의 IPv6 주소를 알고 있는 상태에서, On-Link 목적 노드의 링크 계층 주소를 결정한다.

셋째, 목적지 노드의 실제적인 링크 계층 주소와 라우터의 링크 계층 주소를 확인한다(IPv4의 ARP 기능).

넷째, 노드가 사용하려고 하는 주소를 다른 노드에서 이미 사용 중인지 판단하는 주소 중복을 검사한다.

이와 같은 기능들을 수행하기 위해 RS(Router Solicitation), RA(Router Advertisement), NS(Neighbor Solicitation), NA (Neighbor Advertisement)와

같은 ICMPv6 패킷을 사용하며, 동작 절차는 다음과 같다.

먼저 RS가 각 호스트의 Interface를 이용 가능한 상태로 설정하면, 호스트는 라우터에게 즉시 RA 메시지를 보내줄 것을 요청하게 된다. RA 메시지는 라우터에서 주기적으로 또는 RS 메시지에 대한 응답으로 다양한 링크와 인터넷 매개 변수를 가진 자신의 존재를 메시지를 통해 Advertise 한다. 만약 Multicast가 가능한 링크라면 각 라우터는 주기적으로 RA 패킷을 멀티캐스트하여 자신이 이용 가능한 상태임을 알린다. 이러한 RA 메시지의 전송 주기는 호스트에 의해 수 분 안에 라우터의 존재를 알 수 있도록 충분히 짧으며, 이와 같은 RA 메시지들을 수신한 호스트는 기본 라우터 목록(Default Router List)을 갱신하게 되며, On-link 결정 또는 주소 자동 설정에 사용되는 Prefix 정보 등을 획득 할 수 있게 된다. NS 메시지는 크게 3가지 기능을 수행하는데, 인접노드의 링크 계층 주소를 결정하는 기능, 인접 노드가 저장해 둔 링크 계층 주소를 통해 계속 도달 가능한지 확인하는 기능 및 주소 중복 검사 과정을 위해 사용된다. 먼저 링크 계층 주소를 결정하는 방법을 간단히 보면 노드에 NS 메시지를 보내서 목표 노드에 자신의 링크 계층 주소를 제공하고 동시에 목표 노드의 링크 계층 주소를 요청한다. 즉, 송신 노드는 목표지 노드에게 자신의 링크 계층 주소를 전달하도록 요청하는 NS 메시지를 Multicast해서 주소 해석을 수행하며, 이때 사용되는 목적지 주소는 Target Address 기반의 Solicited-Node Multicast 주소이다. NA 메시지는 일반적으로 NS 메시지에 대한 응답으로 사용되는 메시지이나, NS 메시지를 받지 않은 경우에도 링크계층 주소 변경을 알리기 위한 수단으로도 사용될 수 있다. 이것은 NS 메시지를 받지 않은 상황 하에서도 NA를 전송함으로써 새로운 정보를 신속하게 전파할 수 있다[11].

본 논문의 3장에서는 ICMPv6의 제어 메시지 교환 절차를 기반으로 자동 주소 설정 방식을 제안한다.

2.5 Zero Configuration Networking 기술

기존의 IP 네트워크에서의 주소 설정 방식은 DHCP(Dynamic Host Configuration Protocol) 서버로부터 네트워크 환경을 다운 받아 시스템을 설정하는 방식으로 서버로부터 주소를 할당 받고, 주소 할당에 관한 책임은 전적으로 서버에 있었다. 이로 인하여 대규모의 DB(Data Base)가 필요할 뿐만 아니라, 원격지 서버와의 정보 교환으로 인해 불필요한 망 트래픽을 유발하게 되었고, 또한 TCP/IP 프로토콜에 능숙한 전문적인 관리자들에 의해서만 시스템이 설정되고 유지되었다. 그러므로 이러한 방식은 홈 네트워크, 자동차 네트워크, 비행기 네트워크, 회의장 혹은 임시 응급 센터 등의 ad-hoc 네트워크에서는 효율적이지 못하며, 제한된 네트워크에서 사용자들의 개별적인 요구사항을 모두 만족시키기는 힘들었다. 또한 전문적인 네트워크 관리자가 존재하지 않는 상황에서 독립된 2대 이상의 PC들을 유선 또는 무선망을 통해 연결하는 것도 쉽지가 않다.

따라서 본 논문에서는 이러한 문제점을 해결하기 위한 방안으로 차세대 인터넷 프로토콜인 IPv6를 기반으로 한 자동 주소 설정 방식을 제안하며, 그 프로토콜 규격은 IETF의 Zeroconf 워킹 그룹에서 진행중인 제한 사항을 만족한다.

2000년 3월에 조직된 IETF Zeroconf 워킹그룹은 IP 네트워킹에 필요한 설정이 사용자나 관리자의 관여없이 자동적으로 수행될 수 있게 하는 자동 설정 기술을 연구하고 있다[12][13]. 이러한 기술은 SOHO(Small Office Home Office) 네트워크, 비행기나 기차 같은 교통/운송

수단에서의 네트워크, 정보가전으로 구성된 홈네트워크, 그리고 임시 방편적으로 구성되는 Ad-hoc 네트워크 상에서 IP 네트워킹을 쉽게 운용되도록 고안되었다. 이러한 자동 네트워킹 기술은 Zero-Configuration 또는 Auto-Configuration이라고 명명되는데, 크게 4가지 기술로 구성된다[14].

첫째, IP Interface의 설정. IPv4 Interface 설정은 일반적으로 IP 주소의 할당과 넷 마스크(Net mask)의 설정을 의미하며, 디폴트 라우터와 같은 라우팅 정보를 선택적으로 포함한다. 이러한 IP Interface 설정은 거의 모든 IP 통신을 위해 필요로 하는 기능이며, 송신자와 수신자가 같은 서브넷에 존재하는 경우와 다른 서브넷에 존재하는 두 가지 경우가 있다. 두 경우 모두 한 호스트에서 다른 호스트로 패킷을 전송할 시에는 IP 서브넷을 위한 넷마스크를 정해야 한다. 그리고 IP 서브넷에서의 IP 주소는 유일해야 하고, 인터넷 내에서는 유일한 IP 서브넷을 가져야 한다. 또한 전달되는 패킷에 대한 라우팅 정보를 반드시 라우터들이 유지해야만 한다.

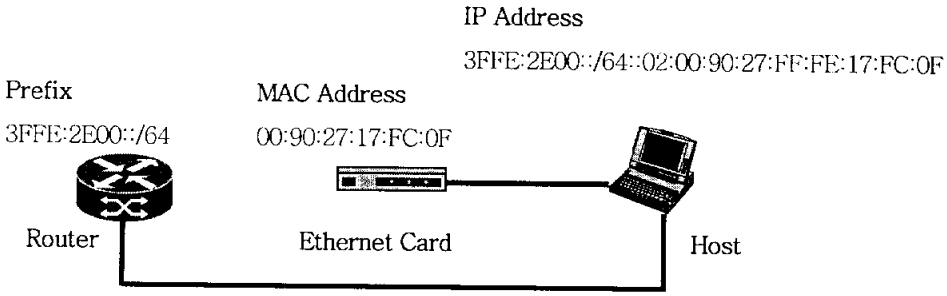


그림2.5 자동 주소 방식(IPv6)

이와 달리, 그림2.5와 같이 IPv6기반 자동 Interface 설정은 IPv6 주소

할당과 Prefix 설정을 의미하며, 이때 라우팅 경로 정보는 IPv6 기본 프로토콜인 ICMPv6의 RA 메시지에 의해 주기적으로 제공되기 때문에 추가적인 프로토콜을 필요로 하지 않는다. IPv4와 마찬가지로 IPv6도 송신자와 수신자가 동일 서브넷에 있는 경우와 그렇지 않는 경우로 나눌 수 있는데, 동일 서브넷에 존재하는 경우에는 NDP에 의해 링크 계층 주소를 얻기만 하면 패킷을 전송할 수 있으며, 다른 서브넷에 존재할 경우에는 먼저 송신자가 패킷을 디폴트 라우터에게 보내고, 그 이후 라우터가 수신한 Prefix 정보에 따라 라우팅 경로를 결정하게 된다. 또한 IPv6 주소체계 내의 범주를 구분하여 동일 링크에서만 사용할 수 있도록 하기 때문에 IPv4 보다는 좀더 효율적으로 사용할 수 있다[11].

둘째, 호스트 이름의 IP 주소로의 변환. 호스트 이름은 사용자가 IP 주소 대신 사용하기 위해 필요하며, 이는 가장 기본적 이면서도 중요한 기능에 해당한다. 웹 브라우저에서 URL 부분은 일반적으로 웹 서버의 이름을 포함하고, 사용자가 URL 부분에 이름을 입력했을 때, 그 이름은 IP 주소로 변환되어야만 실제로 웹 브라우징 기능이 동작하게 된다. 마찬가지로 웹 서버는 사용자의 로그파일을 기록하게 되는데, 이때 IP 주소를 사용자에게 용이한 이름으로 매핑하여 저장하게 된다. 이러한 호스트 이름은 네트워크 상에서 유일해야 하며, 호스트는 자기 자신의 이름이 네트워크 상에서 유일한지를 검사하는 기능을 포함해야 한다. 만약 이름이 유일하지 않으면, 호스트는 이를 사용자에게 통지한 다음 IP Interface 설정 소프트웨어를 통해 새로운 이름을 선택하여 그 이름의 유일성 검증을 반복적으로 수행한다. 이와 같은 호스트 이름과 IP 주소간의 변환 방식은 IPv4와 IPv6가

동일하지만, 128비트의 긴 주소 체계를 사용하는 IPv6에서는 사용자들에게 편이를 제공하기 위해 이러한 기능이 필수적으로 요구된다.

셋째, IP Multicast 주소의 할당. IP Multicast는 수신자 그룹에게 패킷을 전달하기 위해 필요하며, 오디오 및 비디오 또는 뉴스와 같은 응용에 사용된다. 또한 Well-known Multicast 주소들이 논리적인 주소 지정 기능을 위해 사용되는데, 예를 들어, 호스트가 로컬 라우터와의 통신을 요구할 때, 해당 라우터의 IP 주소에 대한 정보가 필요하지 않고, 전체 라우터용 Multicast 주소를 사용하여 패킷을 전송하게 된다. IPv4에서 Multicast를 위해 사용되는 주소 범위는 223.0.0.0~239.255.255.255이며, IPv6의 Multicast 주소는 최상위 8비트가 "ff0"으로 세팅된다. ZeroConf 네트워킹에서 Multicast 주소 할당을 위해서는 로컬, 링크로컬 또는 사이트-로컬 범주 중에서 호스트를 위해 이용 가능한 영역의 목록이 Multicast 응용에게 제공되어야 하며, 동시에 각 영역 당 할당 가능한 주소 범위의 목록이 요구된다.

넷째, 서비스 탐색. 서비스 탐색은 사용자가 미리 알고 있는 이름을 입력하는 것이 아니라 동적으로 발견되는 이름을 사용하여 사용자에게 서비스나 호스트를 효율적으로 선택할 수 있도록 한다. 예를 들어, 간단한 프린터 서비스를 이용하는 경우에 서비스 탐색을 위해 필요한 요구사항은 다음과 같다. 서비스 탐색 프로토콜은 프린터 기능을 필요로 하는 디바이스에 의해 프린터 서비스가 발견될 수 있도록 해야 한다. 이를 위해 서비스 타입이 정의되어야 하며, 동일한 서비스 타입내의 여러 가지 서비스들을 구분하기 위한 서비스 식별자 등을 필요로 한다.

앞에서 기술한 자동 네트워킹의 구성 기술들은 다음 장에서 제안되는 IPv6 환경에서의 자동 주소 설정 방식에 필수적으로 요구되는 사항이다.

3. IPv6 네트워크에서 자동 주소 할당 방안

본 장에서는 앞에서 언급된 IPv6의 특징과 ZeroConf 네트워킹 기술에서의 요구사항들을 기반으로 IPv6 환경에서의 가장 보편적인 주소 지정 방식인 Link-local에서의 주소획득 방식 및 Global and Site-Local에서의 주소획득과 주소 재지정 방식에서의 자동 주소 할당 방안을 제안한다.

3.1 자동 주소 할당 방안

가. Link-local 주소 획득

Link-local 주소는 단일 링크 내에서만 사용가능하며, 경계 라우터가 외부망으로 전파되는 것을 차단한다. 또한, 라우터가 존재하지 않거나 DHCP 서버가 존재한다고 할지라도 적용이 가능하다. 이와 같은 환경에서 생성된 Link-local 주소는 시간적으로 사용상의 제약을 받지 않으며, 단일 링크 내에서는 언제든지 사용이 가능하다.

본 논문에서는 이러한 Link-local 주소에서 특정 서버의 도움없이 주소를 할당함으로써 불필요한 망 트래픽을 줄 일 수 있는 자동 주소 설정 방안을 제안한다.

그림3.1은 주소 생성 과정을 상태 천이도로 나타낸 것이다. 그림에 나타난 주소 생성 과정은 Link-local주소 획득과 다음에 기술될 Global and Site-Local 주소 획득에서도 적용된다. 동작 방식을 살펴보면, 먼저 Invalid 상태에서 Interface ID를 생성할 수 있는 범위에서 임의로 하나를 선택하고, link-local 주소를 위해 할당된 정해진 Prefix(Well-known Prefix)와 결합하여, 링크-로컬 주소를 자동으로 생성하고 Tentative 상태로 천이한다. 그 이후 생성된 임시 주소에 대한 주소 중복 여부를 검출하기

위해 그림3.2에 나타난 DAD(Duplicate Address Detection) 과정을 수행한다. 이때, 먼저 이웃 노드와의 주소 중복 검출을 위해 NS 메시지를 송신한 이후, 그 응답으로 NA 메시지를 수신하여 중복이 검출되지 않을 경우에는 RA 메시지의 Prefix Option에 포함된 Preferred Lifetime 값에 따라 주소의 생성 여부가 결정된다. 하지만 새로운 세션을 설정할 수 없는 주소이거나 유효 생존 기간(Valid Lifetime)을 넘을 경우에는 다시 그림3.1과 같은 절차에 따라 주소를 생성 획득한다.

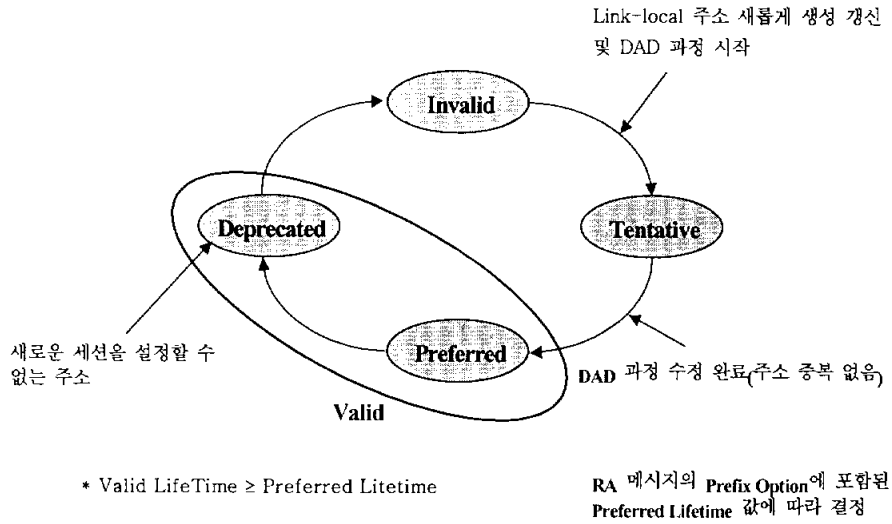


그림3.1 주소 생성 과정

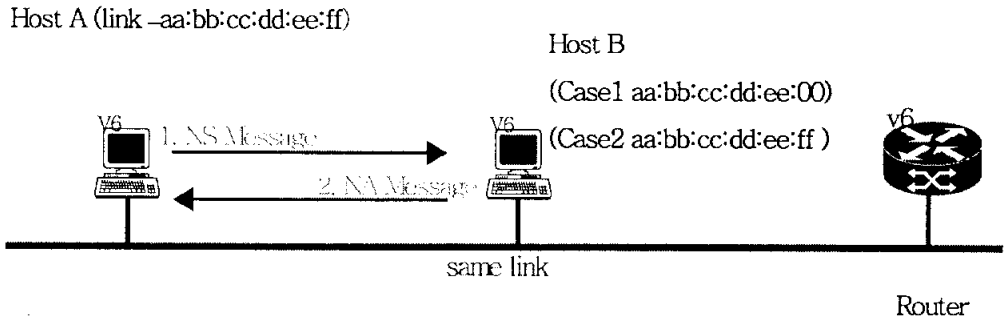


그림3.2 중복 주소 검출 과정(DAD : Duplicate Address Detection)

DAD 과정에 대해 좀더 자세히 살펴보면, 처음 자동으로 생성된 link-local 주소는 링크 내에서 주소의 유일성을 검증 받지 않았기 때문에 임시 주소(Tentative address)라 불리며, 그림3.2와 같은 중복 주소 검출(DAD: Duplicate Address Detection) 과정을 수반한다. 이는 Interface에 주소를 할당하기 이전에 충돌 여부를 검사하는 과정이며, DHCP 서버를 통해 주소를 획득하는 상태 보존형 주소 설정 방식과는 달리 본 논문에서 제안하는 자동 주소 설정 방식에서는 링크-로컬 주소를 생성하기 위해서 DAD 과정이 필수적으로 요구된다.

중복 주소 검출을 위해서 사용되는 메시지는 앞서 2장에서 기술한 ICMPv6의 NS와 NA 메시지를 도입하였다. 먼저 호스트 A에서 임시 주소를 생성한 후 NS 메시지를 네트워크 상으로 보내게 되고, NS 패킷에 대한 응답인 NA 메시지를 기다리게 된다. 이 때, NS 메시지를 송신한 후 그에 대한 응답으로 주소의 중복이 검출되지 않았다는 NA 메시지를 받거나, 일정 시간(Expiration Time)이 지날 때까지 NA 패킷을 받지 못한 경우, 이 주소에 대한 유일성이 검증된 것으로 판단하여 Interface에 주소를 할당한다. 그러나 다른 호스트로부터 중복이 확인된 NA 패킷을 송신한 경우에는 Interface에 그 주소를 할당할 수 없다.

제안된 자동 주소 할당 방식에 의해 할당된 Link-local 주소는 송수신 노드의 주소로 사용될 수 있으며, IPv6 패킷에 그림3.3과 같이 매핑될 수 있다.

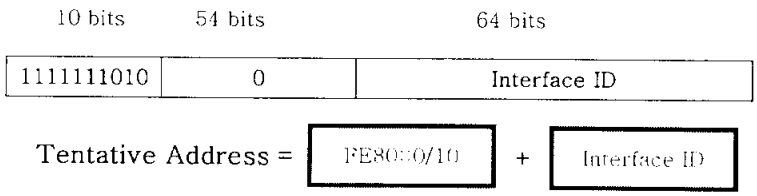
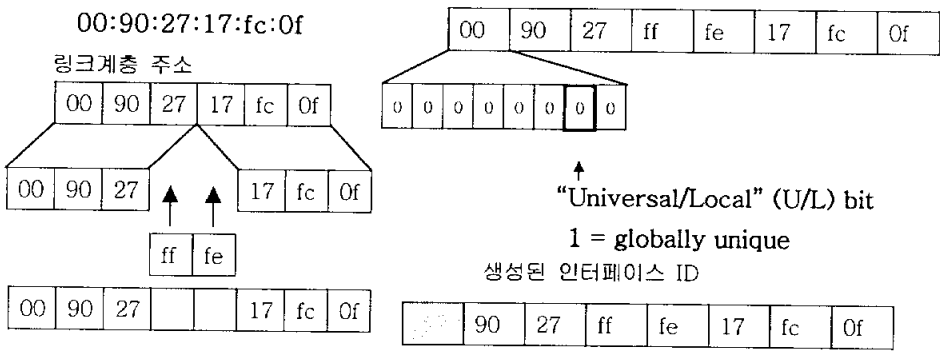


그림3.3 Link-local 주소의 구조

그림3.3의 1111 1110 10(FF80::/10)은 Link-local 용으로 미리 정해진 Prefix(Well-known Prefix)이다. 이것은 각 패킷이 전달될 수 있는 범위를 단일 링크로 제한하기 위해 사용되고, 또한 패킷이 존재하는 네트워크를 식별하기 위해서도 사용된다. 따라서 Well-known Prefix를 이용하면, 라우터로부터 별도의 Prefix에 대한 정보를 획득하지 않고서도 호스트 자신이 Link-local 주소를 생성할 수 있다. 이와 같은 Link-local 주소 설정은 시스템 부팅를 비롯한 다음과 같은 경우에만 요구된다.

- 시스템 구동 시, 네트워크 Interface를 초기화하는 경우
- 일시적인 Interface 오류가 발생한 경우
- Interface가 새로 네트워크에 설치된 경우
- 시스템 관리상 Interface를 일시적으로 정지한 경우, 다시 Interface를 재가동하기 위해 시스템 조작이 필요한 경우

자동 주소 생성 과정에서는 Well-known Prefix 정보에 자신의 Interface ID 정보를 붙여서 생성한다. 이때, Prefix와 Interface ID 사이에는 "0"으로 채워지며, 만일 사용하고자 하는 Interface ID의 비트수가 Prefix 10비트를 제외한 나머지 118비트 이상일 경우에는 주소 생성이 불가능하다. 그러나 IETF에서는 일반적으로 Interface ID로 64 비트를 사용하도록 권고하고 있다[5].

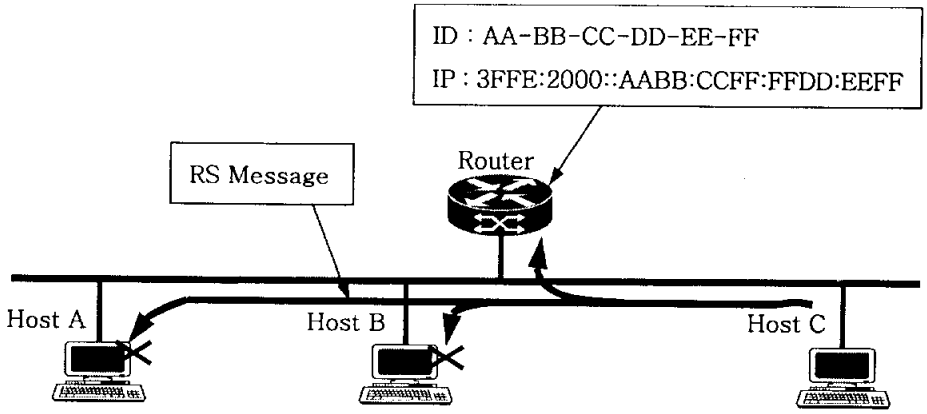


So lower 64 bits in address are 02:90:27:ff:fe:17:fc:0f

그림3.4 이더넷 환경에서의 Interface ID 구성 방법

현재 가장 널리 사용되고 있는 이더넷 환경에서의 자동 주소 설정 방식을 통한 Link-local 주소 설정을 살펴보면, 앞서 언급된 것과 같이 Prefix는 이미 정해져 있고, 링크-로컬 주소를 할당하기 위해서는 나머지 Interface ID를 생성해야 한다. Interface ID를 구성하는 방법은 그림3.4에서 제시된 방법과 같으며, 이더넷 링크-계층 주소가 48비트의 "00:90:27:17:FC:0F"일 경우, Interface ID는 64비트의 "02:90:27:FF:FE:17:FC:0F"가 된다. 여기서, "FF:FE"는 이더넷 환경에서 IEEE EUI-64(Extended Unique Identifier) 형식을 의미하며, 7번째 비트를 "1"로 변경한 것은 Interface ID가 글로벌 범주를 가진다는 의미이다. 이렇게 생성된 Interface ID를 그림 3.3에 나타난 Interface ID 필드에 첨가하면, Link-local 주소가 완성된다.

나. Global and Site-Local 주소 획득

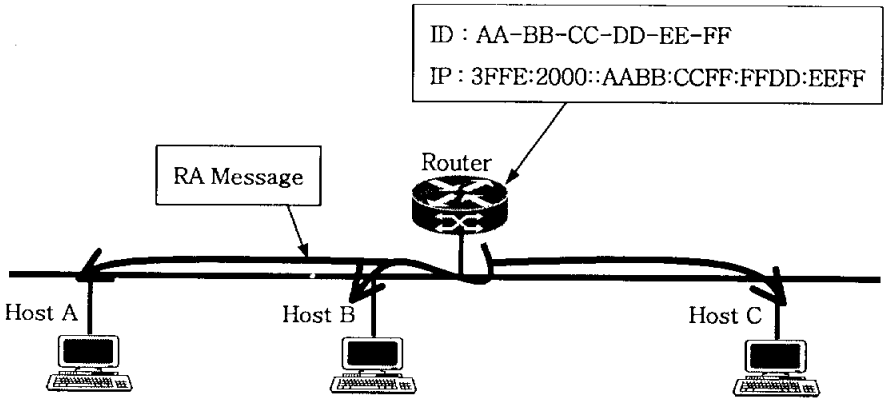


Router Solicitation		
Source Address	FE80::0290:27FF:FE17:FC0F	Sender's link-local address
Destination Address	FF02::1	All-node Multicast address
Option	Source link layer address :00-90-27-17-FC-0F	자신의 링크계층의 주소를 보냄

그림3.5 (호스트→라우트) RS 메시지 전송

Global and Site-Local 주소를 획득하기 위해서는 Prefix가 이미 정해져 있는 링크-로컬 주소의 경우와는 달리 라우터로부터 Prefix와 같은 주소 설정에 필요한 정보가 요구된다.

Global and Site-Local 주소 획득 방식에서도 2장에서 언급된 ICMPv6 패킷을 도입하였으며, 그림3.5에 나타난 것과 같이 라우터에게 주소 설정에 필요한 정보를 명시한 RA 메시지를 송신하도록 호스트 쪽에서 RS 메시지를 보내거나, 그림 3.6과 같이 라우터가 주기적으로 전송한 RA 메시지로부터 획득할 수 있다.



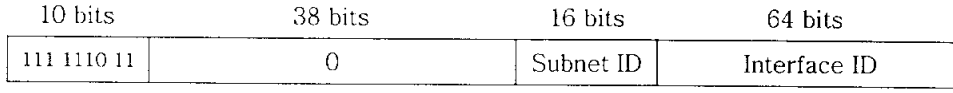
Router Advertisement		
Source address	FE80:AABB:CCFF:FFDD:EEFF	Router의 link-local address
Destination Address	FF02::1	All-node Multicast address
Router Lifetime	10000	라우터로서의 역할 가능 시간(초)
Reachable Time	3600	도달 가능하다 인식하는 시간(초)
Option	AA-BB-CC-DD-EE-FF	자신의 링크계층의 주소를 보냄
	1280	Link MTU 값
	3FFE:2000::/64	Prefix 정보

그림3.6 (라우터→호스트) RA 메시지 전송

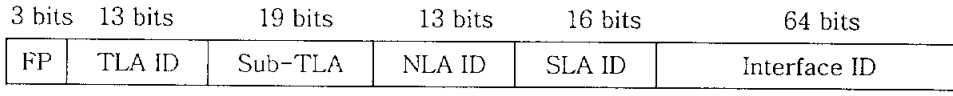
전송된 RA 메시지는 Prefix 정보, 유효 생존 기간(Valid Lifetime), 선호 생존 기간(Preferred Lifetime) 및 호스트의 NA 메시지들의 전송 간격 등과 같은 정보를 포함하며, 호스트는 얻어진 Prefix 정보와 자신의 Interface ID를 이용하여 Site-Locai 또는 Global 주소를 자동으로 설정한다.

주소 생성 과정을 좀더 자세히 살펴보면, 그림3.5에서처럼 먼저 호스트 C에서 RS 메시지를 모든 라우터의 목적지로 보낸 이후, 그림3.6에 나타난 것과 같이 라우터는 주소 설정 정보를 포함한 RA 메시지를

전송하게 된다. 이때, RA 메시지의 목적지 주소는 모든 노드 대상의 Multicast 주소인 FE02::1이다. 이는 RS 메시지를 보낸 호스트 A에 아직 정식으로 할당된 주소가 없기 때문에, 호스트 A가 RA 패킷을 받을 수 있도록 모든 노드로 전송해야 한다. RA 메시지를 수신한 호스트는 RA 메시지의 유효성을 검사한 후 자신의 Interface ID와 수신한 Prefix 정보를 이용하여 주소의 구조에 따라 Site-Local 또는 Global 주소를 생성하게 되며, 획득된 주소를 IPv6 패킷에 매핑하면 그림3.7과 같다.



(a) Site-Local 주소 형식



FP Format Prefix (001)
TLA ID Top-Level Aggregation ID
NLA ID Next-Level Aggregation ID
SLA ID Site-Level Aggregation ID

(b) Global 주소 형식

그림3.7 Site-Local 및 Global 주소 형식

3.2 자동 주소 할당 방식을 이용한 주소 재지정

가. 호스트 주소 재지정

호스트에서의 주소 재지정 기법은 사이트 내에 새로운 호스트를 등록하거나, 전송을 끝낸 호스트를 제거하기 위해 사용된다. 이를 위해, 3.1절에서 제안된 Global and Site-Local에 적용된 자동 주소 설정 기법을 적용하였으며, 동작 절차는 다음과 같다.

먼저 RA 패킷을 통해 새로운 Prefix가 제공되면, 새로운 Prefix에 따라 주소를 구성하게 되고 이전의 Prefix에 의한 주소는 제거된다. 하지만 갑작스런 주소의 제거는 이전의 주소를 이용하여 통신하고 있는 응용들에 대해 에러를 발생시킬 뿐만 아니라, 라우팅 기능도 수행할 수 없다. 따라서 점진적인 주소의 제거를 통해 사용자들에게 미치는 영향을 최소화해야 한다. 이를 위해, 먼저 이전에 사용하던 주소를 Deprecate 주소로 만들고, 유효 생존기간(Vaild lifetime)을 조금씩 줄이면서 일정기간 동안 RA를 전송한다. 여기서 Deprecated 주소는 새로운 세션을 생성할 수 없고, 단지 수신용으로만 사용될 수 있는 주소를 의미한다. 주소들의 상태 변화는 3.1절의 그림3.1의 상태 천이도를 따른다.

여기서 Valid lifetime은 처음 Tentative 상태에서 생성된 주소가 Deprecation 상태로 천이할 때까지의 시간이며, Preferred lifetime은 생성된 주소가 Invalid 상태로 천이할 때까지의 시간이다. 즉, 생성된 주소가 완전히 파기될 때까지의 시간을 나타내며, Valid lifetime이 Preferred lifetime 보다 반드시 길다.

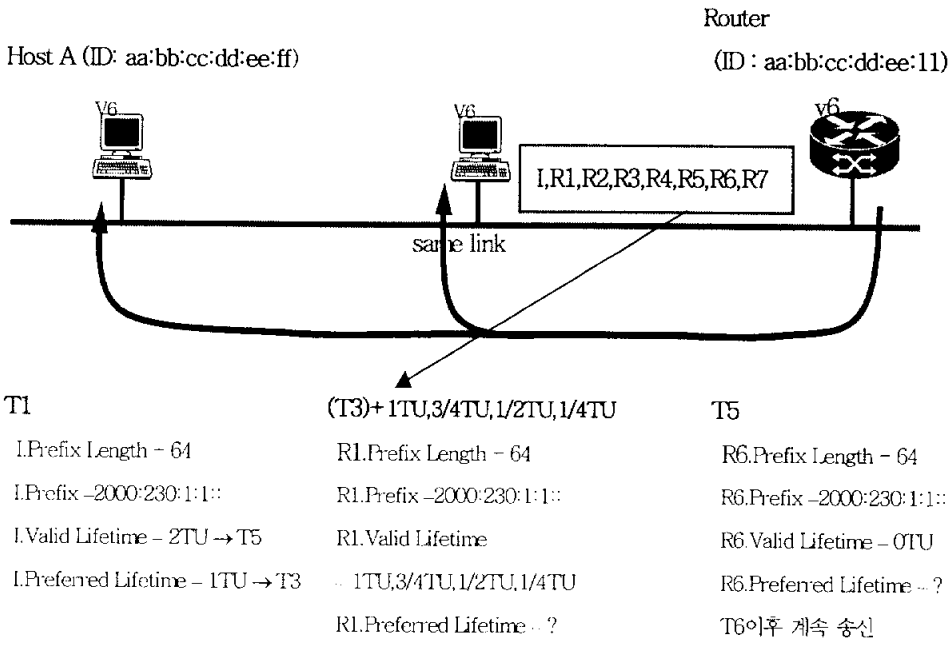


그림3.8 호스트 주소 재지정 예

그림3.8은 앞에서 언급된 호스트 주소 재지정 과정의 예를 나타내며, 동작절차는 다음과 같다. (T1<T2<T3<T4<T5<T6<T7, TU = Time Unit)

첫째, T1 : 라우터는 Prefix A(Valid = 2TU, Preferred = 1TU)를 포함한 RA 패킷을 전송한다. 이때, 특정 호스트가 라우터로부터 RA 패킷을 수신한 후, Unpluged 상태가 된다.

둘째, T3 : Prefix A를 Deprecated 상태로 만들고, T5에는 완전히 Invalid 상태로 만들기 위한 작업을 진행한다. 또한, T2에서 라우터는 주소 재지정을 위한 새로운 Prefix B를 가진 RA 메시지를 전송한다.

셋째, T3 ~ T4 : 이 기간 동안, T2에서 (Valid = 2TU)로 공지했던 Prefix A

에 대한 주소 재지정 과정을 수행한다. 라우터는 Prefix A에 대해, 점점 유효 생존 기간 (Valid lifetime)을 줄이면서 RA 패킷을 전송한다. T4에서는 Prefix A (valid = 0TU , Preferred = 0TU)를 가진 RA 패킷을 전송한다.

넷째, T5 ~ T6 : T5부터는 Prefix A를 가진 주소들은 Invalid 상태가 된다. 따라서 T4에서 호스트 주소 재지정 기간이 끝났으므로, 라우터는 T5이후부터는 Prefix A를 가진 주소들을 라우팅하지 않는다.

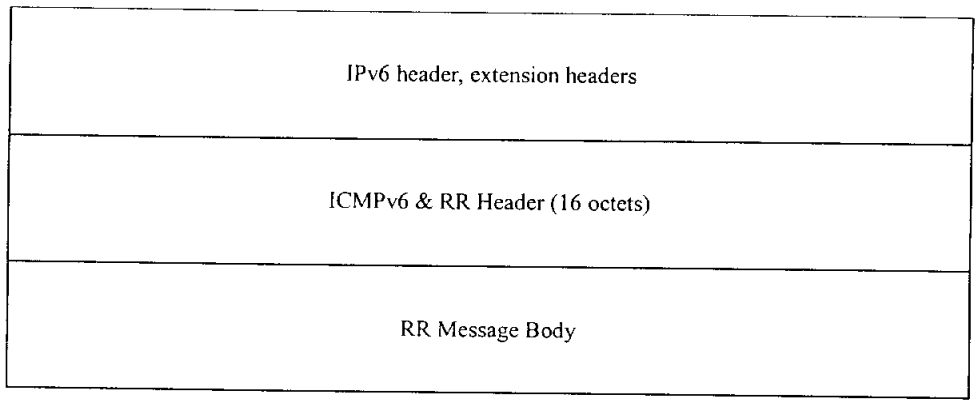
호스트 주소 재지정 과정에서는 유효 생존 기간에 대한 고려가 반드시 요구된다. 왜냐하면, 유효 생존 기간 값이 크게 되면 그만큼 부하가 커지기 때문이다. 예를 들어, 최초 유효 생존기간을 무한대로 설정되면, 무한하게 RA(Valid = 0TU) 패킷을 전송해야 한다. 따라서 이와 같은 불필요한 부하를 줄이기 위해, 가능한 짧은 생존 기간을 가지는 Prefix를 사용해야 한다.

나. 라우터 주소 재지정

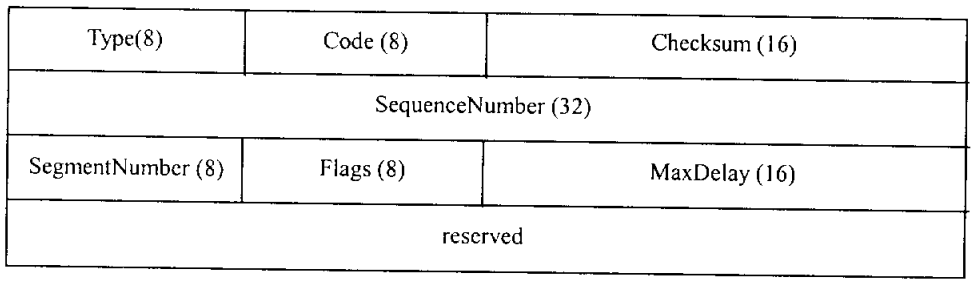
라우터 주소 재지정은 네트워크 내의 호스트 그룹을 관리하는 라우터들을 유지 및 관리하기 위해 필요하다. 라우터 주소 재지정 방식에서도 3.1절에 제안된 자동 주소 설정 방식의 적용이 가능하다.

자동 주소 설정 방식을 이용한 라우터 주소 재지정 방식은 하나의 사이트 내에서 별도의 서버의 도움없이 단지 라우터의 정보만을 가지고 Prefix 정보를 갱신할 수 있도록 해주며, 이를 통해 모든 라우터 상의 Prefix 재설정이 용이하게 된다. 이러한 라우터 주소 재지정 과정에 사용되는 메시지들은 기본적으로 ICMPv6의 패킷 형식을 따르며, 그림 3.9는 라우터 주소 재지정 명령 수행을 위한 메시지 형식을 나타낸다.

주소 재지정 절차를 IPv6의 Command 메시지와 Result 메시지를 도입하였으며, 이러한 메시지들은 그림3.9(a)와 같이 ICMPv6 패킷에 포함되어 전송될 수 있다.



(a) Router Renumbering Message Format



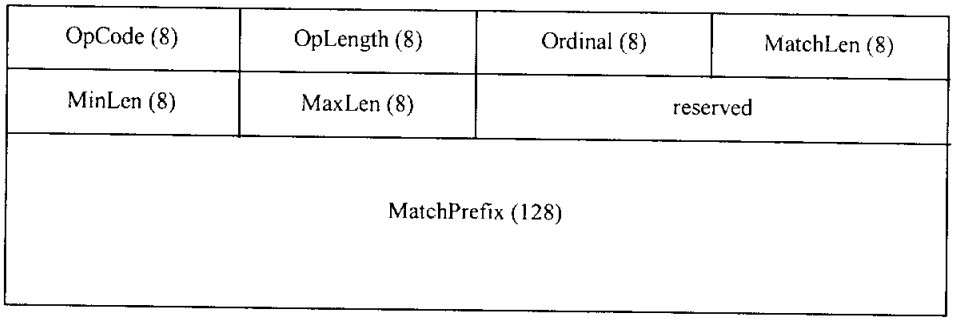
(b) Router Renumbering Header

그림3.9 라우터 주소 재지정 메시지 형식

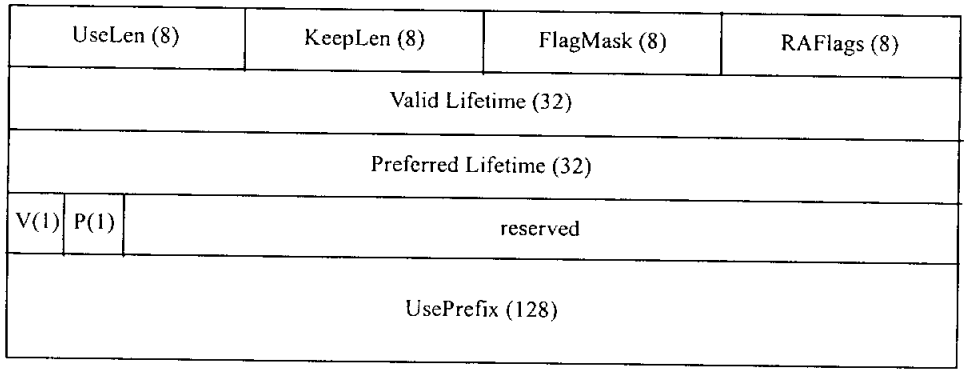
그림3.9(b)에서 라우터 재지정 기능을 수행하기 위해 도입된 IPv6의 RR(Router Renumbering : 주소 재지정) 헤더의 기능은 다음과 같다.

"Type" 필드는 "138"로 세팅되어 라우터 재지정 메시지임을 표시하고, "Code" 필드는 전송된 패킷의 유형(Command : 0, Result : 1)을 나타낸다. "Sequence Number" 필드는 전송되는 메시지의 순서를 표시하며, 재설정 기간 동안에는 그 값이 계속 증가한다. "Segment Number" 필드는

동일한 일련 번호를 가진 서로 다른 유효 RR 메시지를 구분하기 사용되지만, 이 번호에 따라 RR 메시지 간의 순서를 규정하지는 않는다. "Flags" 필드는 T, R, A, S, P등 5가지 비트플래그를 정의 하고 있으며, P 비트를 제외하고 모두 명령 메시지에서 사용된다. 여기서, T 비트는 실제 시험을 위해, R 비트는 송신노드에게 반드시 결과 패킷을 보내달라는 의미로 사용되며, A 비트는 모든 Interface에 적용한다는 것을 의미한다. S 비트는 동일한 사이트에 속한 Interface에만 적용이 가능하다는 것을 나타내며, P 비트는 이전에 처리가 완료된 명령임을 알려주는 비트이다.

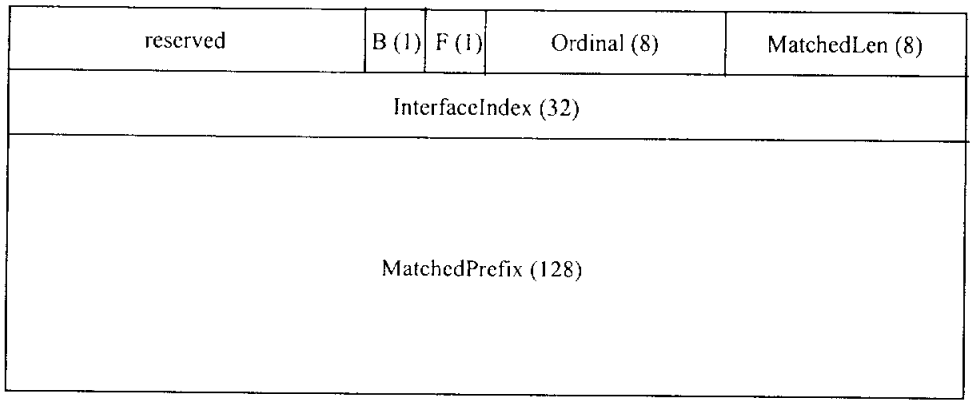


(a) Match-Prefix Part



(b) Use-Prefix Part

그림3.10 라우터 주소 재지정 Command 메시지 형식



Result Message

그림3.11 라우터 주소 재지정 Result 메시지 형식

그림 3.10과 3.11은 라우터 주소 재지정 기능을 수행하기 위해 도입된 IPv6의 Command 메시지와 Result 메시지 유형을 나타낸다.

Command 메시지는 호스트에게 주소 재지정 과정을 수행하기 위해 사용되는 명령들을 명시하며, 호스트의 Interface와의 비교를 위해 사용되는 Match-Prefix 부분과 새로운 Prefix 생성을 위해 사용되는 Use-Prefix 부분으로 나누어진다.

Command 메시지의 Body 필드에 대해 좀더 구체적으로 살펴보면, 각기 가변 길이를 갖는 하나 이상의 PCO(Prefix Control Operation)들로 구성되며, 이러한 PCO들은 OpCode 필드에 따라 실제적인 처리 동작이 수행된다. PCO들의 기능은 Prefix 추가를 위한 ADD, 특정 Prefix 대체와 제거를 수행하는 CHANGE 그리고 사이트 내 모든 Prefix 대체와 제거를 수행하는 SET-GLOBAL로 분류된다. MatchLen 필드에서는 지시하는 길이 만큼의 Prefix 값만이 유효하다는 것을 나타내며, 이 값을 통해 현재 라우터에서 유지되고 있는 Prefix들 중에서 MinLen과 MaxLen 길이에 속한 Prefix들을 비교하여 일치하는 Prefix를 찾게 된다. 그림

3.10(b)의 Use-Prefix 형식에서, UsePrefix 필드는 새로운 Prefix를 결정하기 위해 사용될 수 있으며, UseLen 필드에서는 호스트의 Interface에 대해 새롭게 생성될 Prefix의 초기 비트 수를 명시한다. KeepLen 필드는 새로운 Prefix가 유지해야 할 Prefix 길이를 명시하며, Command 메시지의 나머지 필드들의 정보는 Prefix의 생존주기 및 사용용도에 대한 정보를 명시하기 위해 사용된다.

이와 같은 Command 메시지를 수신한 라우터는 순서에 따라 헤더 검사, 바운드(Bound) 검사, 실행 등 크게 3가지 과정을 수행한다.

먼저 헤더 검사에서는 IPv6의 목적지 노드의 주소, ICMPv6의 전체길이, Code, 순서 번호, 세그먼트 번호 등에 대한 유효성 검사를 수행한다. 다음으로 바운드 검사를 통해 RR 헤더의 T와 R 플래그에 따라 처리 진행 방법을 결정하고, PCO에 포함된 OpCode, OpLenght, MatchLen, MinLen, MaxLen, UseLen과 KeepLen 필드의 값에 따라 이미 정해진 규칙을 준수하는지를 조사한다. 바운드 검사가 끝나면, PCO 값에 따라 순서적으로 새로운 Prefix를 구성하는 작업을 진행한다.

Result 메시지는 Command 메시지에 대한 처리 결과를 전송하기 위해 사용할 수 있다. 먼저 B 플래그를 통해 Command 메시지의 유효성 검사인 바운드 검사의 처리유무를 알려주기 위해 사용되며, F 플래그에서는 PCO에 포함된 Use-Prefix 내에 Multicast나 루프백 주소와 같은 금지된 주소들이 포함되어 있음을 지시한다. MatchedPrefix 필드를 이용하여 일치된 Prefix 정보가 MatchedLen 길이 만큼 유효하다는 것을 명시하며, 또한 이 Prefix 값으로 설정된 Interface를 식별하기 위해 Prefix 값을 InterfaceIndex에 표시한다.

라우터 주소 재지정 기능을 수행하기 위한 절차는 다음과 같다.

첫째, 상위 라우터는 하위 라우터에게 Command 메시지를 전송하여 Prefix 재설정을 지시한다. 이때 메시지 내에 하위 라우터가 처리해야 할 사항(Prefix Control Operation : ADD, CHANGE, SET-GLOBAL)과 하위 라우터의 Prefix(Match-Prefix)를 명시한다.

둘째, 각 라우터들은 사이트상의 상위 라우터가 전송한 Command 메시지에 명시된 Match-Prefix와 자신의 Interface가 일치하는지를 검사한다.

셋째, 자신의 Interface와 Command 메시지에 명시된 Match-Prefix와 일치한 라우터는 Command 메시지의 PCO 즉, Prefix의 삽입(ADD), 제거(CHANGE), 대체(SET-GLOBAL) 명령을 수행한다.

그림3.12에서 실제 라우터 주소 재지정 과정에서 Command 메시지의 설정 예를 보여주며, 하나의 서브넷에 대한 주소 재지정 예를 나타낸 것이다.

IPv6 헤더

Next Header = 58 (ICMP)

Source Address = (관리 노드 주소)

Destination Address = FF05::2 (사이트 로컬 범주의 모든 라우터용 멀티캐스트 주소)

ICMPv6 FR 헤더

Type = 138 (라우터 주소 재지정) Code = 0 (명령코드)

Flage = 60 Hex(R, A)

First(and only) PCO

Match-Prefix Part

Opconde = 2 (변경 작업 코드)

OpLength = 11 (Use-Prefix 영역이 두 개임을 알 수 있음)

Ordnel = 0 (임의의 값 2)

Matchlen = 64

MatchPrefix = Old 64 프리픽스

① 이전 프리픽스의 보존

First Use-Prefix = Part

UseLen = 0

KeepLen = 64 (This retains the oldprefix value intect)

FlagMask = 0, RAFlags = 0

ValidLifetime = 28800 seconds (8 hours)

Preferred Lifetime = 7200 seconds (2 hours)

V flag = 1 , P flag = 1

UsePrefix = 0::0

Second Use-Prefix Part

② 새로운 프리픽스 정의

UseLen = 64

KeepLen = 0

FlagMask = 0, RAFlags = 0

Lifetimes V & P flags - as desired

UsePrefix = New/64 프리픽스

그림3.12 라우터 주소 재지정 Command 메시지 예

4. IPv6 네트워크에서 ZeroConf에 기초한 Multicast 주소 할당 방안

Multicast 전송의 기본 개념은 송신자가 원하는 수신자들에게 데이터 패킷을 전달하는 것이 아니라 데이터를 요구하는 수신자들이 특정 Multicast 주소를 이용하여 해당 Multicast 그룹에 합류하는 소위 수신자 위주의 데이터 전송 방식이다. 이러한 Multicast 통신에서는 다수의 호스트들이 동시에 데이터 전송에 참여하여 네트워크 내에 대량의 트래픽이 전송되며, 상대적으로 각 시스템에서의 부하도 유니캐스트 환경보다 상당히 크다. 따라서 각 호스트에서의 신속한 처리 절차가 요구되고, 또한 대량의 트래픽이 전송되는 상황 하에서 사용자에 대해 신뢰성있는 서비스를 보장해 줄 수 있어야 한다.

그러나 기존의 연구들은 이러한 Multicast 통신 환경하에서 송신자와 수신자에 대한 데이터 전송 및 이에 대한 제어 기법을 함께 다룸으로써 각 시스템에서의 처리 부담을 증가시킬 뿐만 아니라 그로 인한 신속하고, 신뢰성있는 Multicast 통신이 힘들었다.

본 논문에서는 이러한 문제를 해결하기 위한 방안으로, IPv6 기반의 Multicast 통신망에서 Multicast 주소 획득을 위해 ZMAAP(Zeroconf Multicast Address Allocation Protocol)를 도입하고, 이를 3장에서 제안된 자동 주소 할당 방안에 적용하여 IPv6 기반에서 체계적인 그룹 관리를 통한 효율적인 자동 Multicast 주소 할당 방안을 제시하고자 한다.

4.1 ZMAA 프로토콜의 호스트 그룹 관리 체계

Multicast 통신에서는 다수의 호스트들이 하나의 라우터 혹은 네트워크 상의 다수의 라우터에 분산되어 일련의 호스트 그룹을 형성한다. 또는 특정 호스트가 한 개 이상의 호스트 그룹의 구성원으로 참여하여 자신이 속한 호스트 그룹에서 데이터를 전송할 수 있다. 따라서 이러한 복잡한 구조의 환경에서는 호스트 그룹 내의 모든 호스트들에 대해 메시지 전달 및 관리가 효과적으로 제공되어야 하고, 또한 신속하고 신뢰성있는 Multicast 서비스가 제공되어야 한다.

ZMAA 프로토콜은 이러한 문제들을 해결하기 위한 효과적인 방식으로, 체계적인 관리 메커니즘을 제공한다.

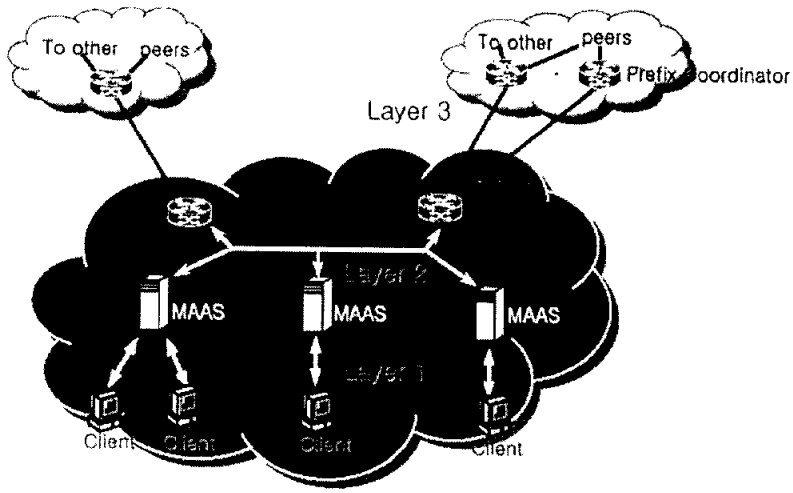


그림4.1 ZMAA 프로토콜의 호스트 그룹 관리 체계

그림4.1은 ZMAA 프로토콜의 계층적인 호스트 그룹 관리 체계를 나타내며, 각 계층별 기능은 다음과 같다.

첫째, Layer 3은 하나 혹은 그이상의 라우터 즉, 호스트 그룹으로 구성된 집단이며, 구성원은 서로 다른 라우터상에 존재 할 수도 있다. 호스트 그룹은 Multicast 통신에서 하나의 논리적인 엔티티로 취급되며, 다음에 언급될 Layer 1 계층이 호스트별 Multicast 서비스를 제공한다면, Layer 3은 라우터 레벨에서의 Multicast 전송을 담당한다. 따라서 Layer 3 계층은 다수의 호스트들로 구성된 호스트 그룹의 생성, 삭제, 수정과 주소 할당 범위 규정 등의 효율적인 관리 기능을 제공하여, 호스트간 효율적인 통신 서비스를 제공한다.

둘째, Layer 2는 호스트 그룹 내에서 개별 호스트가 요구하는 Multicast 전송 서비스를 제공하기 위해 그룹내에서 할당할 수 있는 Multicast 주소를 유지, 관리하는 기능을 담당한다. 이를 위해, 상위 계층의 정보를 이용하며, 또한 상위 계층과 상호 연동하여 중복된 주소 할당을 피하기 위한 주소 범위를 배정한다. 이때, 네트워크 상의 클라이언트들에게 Multicast 주소 할당 서비스를 제공하는 노드로 MAAS (Multicast Address Allocation Server)를 이용한다. 그러나 MAAS는 주소 할당 정보를 유지, 관리하는 별도의 서버가 아니며 네트워크 내의 라우터들이 이 기능을 수행한다.

셋째, Layer 1에서는 소수의 서버들이 다수의 호스트들에게 실제 Multicast 주소를 배정하는 기능을 수행하며, 3장에서 제안된 자동 주소 할당 방안을 토대로 효율적인으로 Multicast 주소 배정 기능을 수행할 수 있다.

위에 언급된 ZMAA 프로토콜의 계층을 기능을 통해, Multicast 서비스를 위해 신속하고 신뢰성 있는 메시지 전달 및 관리가 효과적으로 제

공될 뿐만 아니라, 호스트 그룹 및 호스트 그룹 내의 모든 호스트에 대한 관리가 체계적으로 이루어질 수 있다.

4.2 ZeroConf에 기반한 Multicast 주소 할당 방안

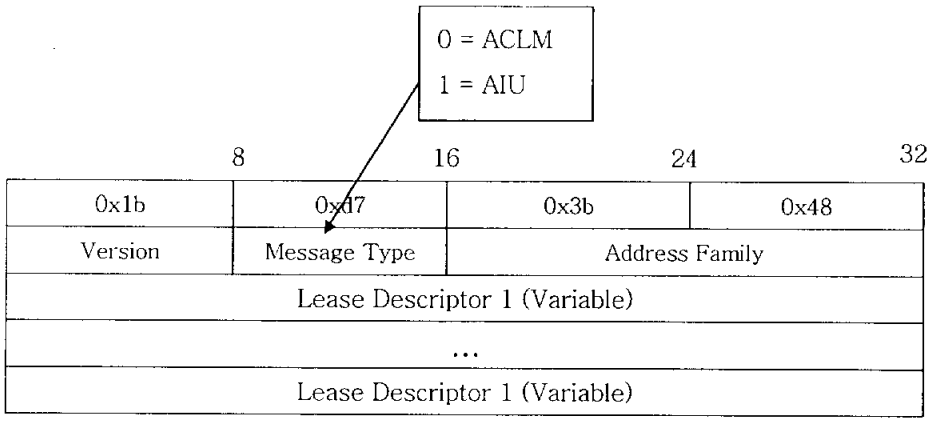
본 절에서는 3장에서 제안된 자동 주소 할당 방식을 적용하여, ZMAA 프로토콜의 layer 1에서의 실질적인 주소 배정을 위해 사용될 수 있는 효율적인 Multicast 주소 할당 방안을 제안한다.

ZMAA 프로토콜은 같은 호스트 상에서 동작하는 어플리케이션에게 Multicast 주소 배정을 담당하는 mini-MAAS가 효율적인 Multicast 주소 배정을 가능하게 해주는 peer-to-peer 프로토콜이다.

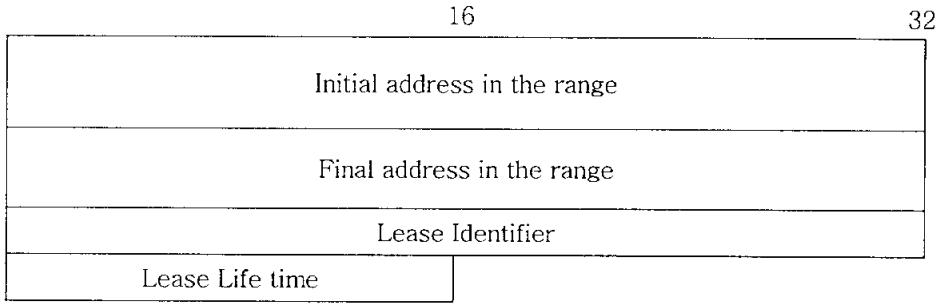
본 논문에서는 mini-MAAS의 주소 배정 과정에 자동 주소 할당 방식의 DAD 개념을 도입하여, Multicast 주소의 중복을 회피함으로써 신뢰성 있는 Multicast 주소 할당 방안을 제안한다.

Multicast 주소 획득에 필요한 정보를 교환하기 위해 기존의 mini-MAAS가 사용하는 ZMAAP 메시지 형식을 도입하였다. ZMAAP 메시지는 message type 필드의 값에 따라 ACLM(Address Claim) 메시지와 AIU(Address In Use) 메시지로 구분되는데, 이 중 ACLM 메시지는 Multicast 서비스를 위한 주소 요구를 위해 사용될 수 있으며, AIU 메시지는 현재 요구한 메시지에 대한 사용 여부를 알리기 위한 기능으로 사용될 수 있다.

그림4.2는 IPv6 기반에서 Multicast 주소 획득을 위해 도입된 ZMAAP 메시지 형식을 나타낸다.



(a) ZMAAP Message Format



(b) IPv6 Lease Descriptor Format

그림4.2 ZMAAP Message Format

그림4.2(a)에서 처음 4바이트는 mini-MAAS가 동작하는 Multicast 그룹과 포트에서 일어나는 프로토콜 충돌을 검출하기 위한 기능을 위해 사용되고, 이를 'magic number'라 하며, magic number로 시작하지 않는 메시지들은 모두 삭제한다. 그리고 다음의 Version 필드는 ZMAAP의 버전을 나타내며, Message Type 필드는 ACLM(Address Claim) 메시지(value=0)와 AIU(Address In Use) 메시지(value=1)로 구분하는 기능을 담당한다.

Lease descriptor 필드들을 이용하여, 주소 자동 설정 방식에 사용될 수 있는 Multicast 주소의 범위를 명시할 수 있으며, 세부적인 형식은 그림4.2(b)와 같다.

그림4.2(b)에서 Initial address in range 필드와 Final address in range 필드는 자동 주소 할당을 통해 요구되거나 배정된 주소의 범위를 명시하기 위해 사용될 수 있다. Lease Identifier 필드는 동일한 주소 범위에서 주소를 할당하는 mini-MAAS들을 구분하기 위해 사용된다. 마지막으로 Lease Lifetime 필드는 메시지가 수신된 이후 주소의 범위가 캐쉬메모리에 유지되는 시간을 초단위로 나타낸다.

ZMAAP 메시지에 포함되는 Lease descriptor들의 수는 Message type에 의해 최대 Payload값에 따라 결정된다. 최대 payload는 1280byte 이며 Maximum Payload 값을 초과하면, 여러 개의 ZMAAP 메시지를 이용한다.

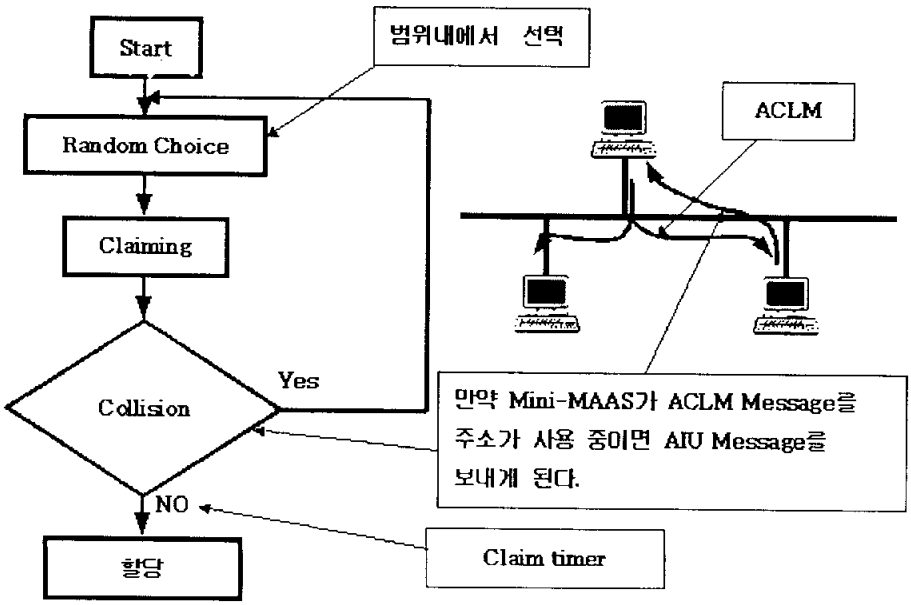


그림4.3 Multicast 주소 할당 메커니즘

그림4.3은 주소 자동 할당 방식이 적용된 Multicast 주소 할당 메커니즘을 나타내며, 세부적인 동작절차는 다음과 같다.

1. 사용자 응용 프로그램은 Local Mini-MAAS에게 주소의 범위(주소의 number와 scope 명세)를 요청
2. Mini-MAAS는 Multicast 주소 범위를 랜덤하게 선택
3. local mini-MAAS는 다른 mini-MAAS들에게 ZMAAP ACLM(Address Claim) 요청 메시지를 전송하여 랜덤하게 선택된 범위의 Multicast 주소를 요구
4. mini-MAAS는 현재 사용중인 경로의 배정과 충돌을 검출
   (주소 할당 과정에서의 혼잡 상황에 대한 대처 가능 - 3.1절의 DAD 개념 도입)
5. 충돌을 알리는 AIU(Address In Use) 응답 메시지를 local mini-MAAS로 전송
6. AIU 응답 메시지 수신시 새로운 주소 범위 선택
7. 만약 Timer out 까지 AIU 응답 이 없으면, Multicast 주소 범위 선택 성공

mini-MAAS는 위의 절차를 통해 할당된 Multicast 주소 범위를 유지하기 위해, 다른 서버에 의해 같은 범위의 주소를 요구하는 ACLM 메시지가 수신되었을 경우, 그 즉시 AIU 응답 메시지를 전송하여 충돌을 보고한다. 또한, 효율적인 주소 자원 관리를 위해 주소 범위 배정 정보를 일정한 lifetime 동안만 유지한다.

그림4.4는 Multicast 주소 할당 과정 종료 후, IPv6 패킷 형식에 적용한 Multicast 주소 형식을 나타낸다.

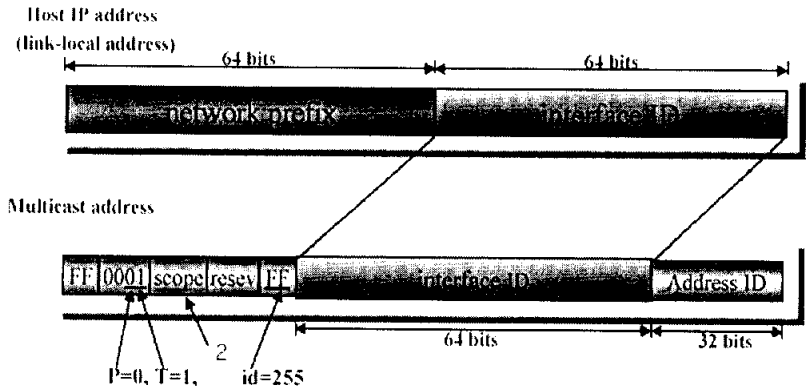


그림4.4 IPv6 기반의 Multicast 주소 형식

본 논문에 제안된 Multicast 주소 할당 방식에서는, 대량의 트래픽이 전송되는 Multicast 환경의 주소 할당 과정에서 야기될 수 있는 혼잡 상황을 주소 관리를 위한 추가적인 서버의 설치없이, 자동 주소 설정 방안을 도입함으로써 해결하였다. 그리고 제안된 자동 주소 할당 방식을 통해, 원격지의 서버와 호스트 사이에서 주소 획득을 위한 정보를 교환하기 위해 사용되는 불필요한 망 트래픽 문제를 해결할 수 있다.

5. 결 론

초기에 단지 연구 망으로 사용되던 인터넷이 폭넓은 컴퓨터의 보급에 의해 표준 통신 프로토콜로 등장하게 되었고, 이로 인해 인터넷 사용자가 급격히 증가했을 뿐만 아니라, 사용자 요구 사항도 다양하게 변화하였다. 이러한 상황에서 기존의 IPv4 기반의 인터넷은 주소 부족, 네트워크의 속도 저하, 멀티미디어 서비스 미흡, 보안 등의 다양한 문제에 직면하게 되었고, 이러한 문제들을 해결하기 위한 새로운 방식의 도입이 절실하게 요구되었다.

따라서 변화하는 네트워크 환경에 효율적으로 대처하기 위한 방안으로 IETF에서는 IPv6를 차세대 인터넷의 핵심 기술로 규정하였으며, 또한 현재 IPv6 기술을 상용화하기 위한 노력이 범세계적으로 활발하게 진행되고 있다.

본 논문에서는 이러한 IPv6 기반의 네트워크에서 IP 네트워킹에 필수적인 설정 및 서비스를 자동화하는 Zero-Configuration 개념을 도입하여 자동 주소 할당 방안과 이를 이용하여 누구나 쉽게 Multicast 서비스를 이용할 수 있는 Multicast 주소 할당 방안을 제시하였다.

이를 위해, IPv6 및 Zero-Configuration networking 기술을 소개하였고, IPv6 기반의 네트워크 환경에서 Zero-Configuration 개념을 도입하여 주소 자동 설정 방안을 제안하였다. 그리고 이러한 주소 자동 설정 방식을 적용하여 Multicast 상황에서의 자동 주소 할당 방안과 Multicast 환경의 주소 할당 과정에서 야기될 수 있는 혼잡 상황에 대한 대처 방안을 제시하였다.

향후 연구 방향으로는 사용자 서비스 요구 사항을 면밀히 분석하여, 개별 망에서 Multicast 기법을 활용하는 다양한 응용서비스 기술 개발

이 필요하며, 또한 네트워크의 하부 구조 단순화를 통해 사용자에게 더욱 더 신속하고 신뢰성 있는 서비스 제공에 대한 연구가 진행되어야 한다.

참고 문헌

[1] S. Deering and R. Hinden. "Internet Protocol version 6(IPv6) Specification," RFC 2460, 1998, 12

[2] "IPV6: The new internet protocol", Huitema Christian, prentice Hall DTR

[3] F.Kastenholz. "IP the next generation," RFC 1762, 1994, 12

[4] R. Hinden and S. Deering. "IP Version 6 Addressing Architecture," RFC 2373, 1998, 7

[5] R. Hinden and S. Deering. "An IPv6 Aggregatable Global Unicast Address Format," RFC 2374, 1998, 7

[6] IETF, Http://www.ietf.org

[7] IPv6 Forum, Http://www.IPv6forum.com

[8] 전 세계 IPv6 공식 주소 할당 현황, Http://www.dfn.de/service/ipv6 /ipv6aggis.html

[9] J.Postel. "Internet Control Message Protocol DARPA Internet Program Protocol Specification" RFC 792 1981, 9

[10] A. Conta and S. Deering. "ICMP for the Internet Protocol Version 6(IPv6)," RFC 2463, 1998, 12

[11] T. Narten E. Nordmark and W. Simpson. "Neighbor Discovery for IP version 6(IPv6)," RFC 2461, 1998, 12

[12] Zero Configuration Network. Http://www.ietf.org/html.charters/zeroconf-charter.html

[13] ZeroConf WG. Httpd://www.zeroconf.org

[14] M. Hatting, Editor. Intel Corp, "draft-ietf-zeroconf-reqts-09.txt," 2001. 8

[15] "TCP/IP Protocol Suit", Forouzon and Behrouz A, McGrow-Hill

감사의 글

지금껏 유형무형으로 내게 도움을 준 고마운 분들게 감사의 글을 드리고자 합니다.

늘 늦게 들어오는 자식을 기다리고 계시는 자상하신 어머님께 키워주시고, 길러주시며, 오늘날에 저를 있게 해 주셔서 감사 드립니다.

본 논문발표회에 친히 참석하시어 도움을 주셨던 김 석태 교수님, 윤 종락 교수님, 정 연호 교수님, 박 규칠 교수님 그리고 친히 논문심사를 맡아주셨던 하 덕호 교수님, 장 주석 교수님, 그리고 학문에의 뜨거운 열의와 강한 트레이닝으로 제자들에 대한 애정을 느끼게 해 주셨던 자상하신 김 성운 교수님께 깊이 고개 숙여 감사 드립니다. 석사시절동안 많은 가르침을 주신 모든 교수님들에게도 감사의 마음을 전합니다.

함께 공부하며 서로 의지하며 보냈던 대학원 동료 선후배 여러분들 그리고 논문을 쓰면서 수정 상황과 논문의 진행과정을 같이 의논해준 신 주동 , 배 정현 , 윤 미라 씨의 따뜻한 배려에 감사 드리며, 송 현수의 아낌없는 협조에 감사 드립니다.

이밖에도 저를 아는 모든 분들게 이제까지의 제 삶에 영향을 준 것에 대해서 깊은 감사의 마음을 전하며, 항상 건강하시고 웃음을 잃지 않으시길 바랍니다.