Journal of Korea Multimedia Society Vol. 14, No. 1, January 2011(pp. 144-152)

IPv6 환경에서 호스트 탐색 및 네트워크 접속 차단 에이전트 시스템

정연기†, 문해은††

요 약

IPv4 주소가 고갈되어가고 있기 때문에 IPv6 주소의 사용이 늘어나고 있다. IPv6 환경에서는 주소자동설정 기능이 제공된다. 주소가 각 호스트(host)에 자동으로 할당될 경우, 네트워크 관리 시스템은 모든 장비의 IP주소를 조사하고 해당 정보를 유지해야 하는 어려움이 따른다. 또한, IP주소가 자동으로 설정되기 때문에 악의적 사용자가 아무런 제약 없이 네트워크 주요장비에 접근할 수 있는 문제가 발생한다. 이런 문제를 해결하기 위해 악의적 사용자들에 대한 관리 및 차단이 필요하다. 본 논문에서는, IPv6 환경에서 호스트를 탐색하고 인가되지 않은 호스트가 네트워크에 접속하는 것을 차단함으로써, 네트워크 주요 자원을 효율적으로 관리하고 보호하는 호스트 탐색 및 네트워크 접속 차단 에이전트 시스템을 제안한다. IPv6 환경에서 본 에이전트 시스템의 성능을 테스트한 결과, 본 시스템은 정상적으로 탐색과 차단 기능을 수행하였다.

An Agent System for Searching of Host Computer and Blocking Network Access in IPv6 Environment

Younky Chung†, Haeeun Moon††

ABSTRACT

As IPv4 addresses are exhausting, the use of IPv6 addresses is increasing. IPv6 environment provides address auto-configuration function. If addresses are allocated to each host automatically, network management system has difficulty in inspecting every IP of all devices and keeping the relevant informations. Also, as IP addresses are configured automatically, problems such as malicious users accessing network devices with no restriction can occur. To solve these problems, managing and blocking of malicious user is necessary. In this paper, we suggest agent system for searching of host computer and blocking network access which manages and protects the major network resources efficiently by searching host and blocking unauthorized host access to network in Ipv6 environment. According to the test results of function of this agent system in IPv6 environment, we have checked that this system performs searching and blocking function normally.

Key words: IPv6, Duplicate Address Detection(중복된 주소 탐색), Host Search(호스트 탐색), Blocking of Access(접속 차단)

1. 서 론

32비트 주소체계인 IPv4의 고갈이 점차 현실화 되어가고 있다. 한국인터넷 진흥원 IPv6포탈의 자료에 의하면 2011년에는 IPv4 주소가 고갈될 것이라고 예측하고 있다. 주소고갈을 인지한 많은 기업 및 관공

※ 교신저자(Corresponding Author) : 정연기, 주소 : 경북 경산시 하양읍 부호리 경일대학교 컴퓨터공학부(712-701), 전화 : 053)850-7286, FAX : 053)850-7280, E-mail : ykchung@kiu.ac.kr
접수일 : 2010년 10월 4일, 수정일 : 2010년 10월 28일
완료일 : 2010년 11월 4일
† 종신회원, 경일대학교 컴퓨터공학부 교수
†† 준회원, (주)넷맨 수석연구원/연구소장
(E-mail : mayfly74@netman.co.kr)

서에서는 이미 IPv4 네트워크에서 IPv6 네트워크로의 전환사업을 진행하고 있어 IPv6를 사용하는 수요가 점점 늘고 있는 추세이다[1,2].

IPv6 네트워크 환경에서는 IP주소의 자동설정을 지원하는데, 이렇게 자동으로 주소가 할당 될 경우 네트워크의 자원을 관리하는 측면에서는 모든 장비의 IP를 확인하고 해당 정보를 유지해야 하는 어려움이 따른다. 또한, IP주소가 자동으로 설정되기 때문에 악의적 사용자가 아무런 제약 없이 네트워크 주요 장비에 접근할 수 있는 문제가 발생한다. 이런 사용자들에 대한 관리 및 차단이 필요하다.

본 논문에서는, IPv6 환경에서 호스트를 탐색하고 인가되지 않은 호스트가 네트워크에 접속하는 것을 차단하여, 네트워크 주요 자원을 효율적으로 관리하고 보호함으로써 한 단계 높은 보안환경을 구축할 수 있는 방안을 제안한다.

IPv6에서 호스트의 탐색 및 차단을 위해서 NDP (Neighbor Discovery Protocol)를 이용한다. 호스트의 탐색을 위해 NS(Neighbor Solicitation) 패킷을 이용하여 탐색하려는 호스트에게 링크계층 주소(link layer address)를 요청하고, 해당 호스트가 NA (Neighbor Advertisement) 패킷으로 응답하면 탐색 리스트를 갱신하여 수신된 링크계층 주소 정보를 유지한다. 그리고 특정 호스트의 차단을 위해 관련된 정책을 설정한 후, 네트워크에서 감지되는 NDP 패킷을 분석하여 정책에 포함되어 있는지 여부를 확인하고, 포함되어 있으면 변조된 NA를 이용하여 해당 호스트를 차단하게 한다.

서론에 이어 2장에서는 IP 주소의 자동 설정 동작에 대해 분석하고, 3장에서는 호스트 컴퓨터 탐색 및 접속 차단을 위한 에이전트 시스템의 설계 및 구현 방법에 대해 설명한다. 4장에서 구현 결과를 분석하고, 5장에서 결론을 맺는다.

2. IPv6 환경에서 IP주소 자동설정

2.1 ICMPv6

ICMP(Internet Control Message Protocol)는 네트워크 상태에 대한 메시지를 주고받을 수 있도록 동작하며 IP와 동일한 네트워크 계층에서 동작한다.

ICMPv6는 IPv6에서 사용되는 ICMP이다. 그림 1에서 보는 바와 같이 기본적인 기능은 ICMP와 동일

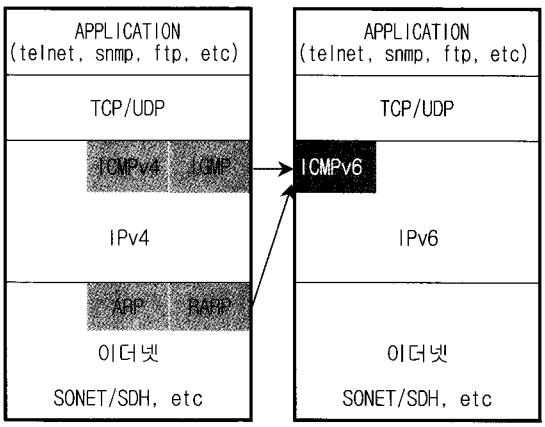

그림 1. ICMPv4와 ICMPv6의 비교

하며 IPv4에서 사용되던 프로토콜인 ARP(Address Resolution Protocol), RARP(Reverse Address Resolution Protocol), IGMP(Internet Group Management Protocol)가 ICMPv6에 포함되어 있다[2-5].

2.2 NDP(Neighbor Discovery Protocol)

NDP는 IPv6환경에서 인접 호스트와 통신을 하기 위해 사용되는 프로토콜로 ICMPv6에 포함되어 IPv4환경에서 ARP가 수행하는 기능을 대신한다. NDP의 주요기능은 표 1과 같다[4,6]. NDP의 주요기능을 구현하기 위해 표 2에 보인 바와 같은 패킷을 사용한다.

2.3 주소의 자동설정

IPv6에서는 일반 사용자가 인터넷에 접속할 때, 128bit의 복잡한 IPv6 주소를 직접 설정하지 않아도

표 1. NDP의 주요기능

기 능	설 명
Router and Prefix Discovery	호스트는 RS와 RA 메시지를 이용하여 네트워크에 존재하는 라우터를 발견하고 해당 네트워크의 prefix정보를 수신함.
Address Resolution	IPv6의 NDP에서 IPv4의 ARP 기능을 대신한다. 호스트는 NS와 NA 메시지를 이용해서 인접 노드의 링크계층 주소를 조사한다.
Redirect	IPv4의 redirect메시지의 기능과 동일. 여러 개의 라우터가 존재하는 네트워크에서 기본 라우터 외에 다른 라우터를 통해 데이터를 전송할 때 사용하는 메시지

표 2. NDP 패킷의 종류와 용도

구 분	설 명
RS(Router Solicitation)	호스트가 빠른 네트워크 정보 획득을 위해 RA정보를 요청하는 패킷
RA(Router Advertisement)	라우터가 자신의 정보를 호스트에게 알려주는 패킷. 자신의 링크계층주소, IP, prefix, MTU정보를 호스트에게 제공. RA패킷은 주기적으로 multicast IP로 제공되며, RS패킷의 요청에 응답하여 수시로 제공된다.
NS (Neighbor Solicitation)	호스트가 주변 호스트와 통신하기 위해 링크계층주소 정보를 요청하는 패킷. IP를 구성한 후 해당 IP가 네트워크에 이미 사용 중인지 아닌지 확인하기 위해 DAD (Duplicate Address Detection)를 사용하기도 함.
NA (Neighbor Advertisement)	NS의 요청에 응답하여 보내지거나, 호스트가 자신의 정보(링크계층주소, 라우터 동작유무)를 빠르게 전파하기 위해 multicast IP로 제공되는 패킷
Redirect	네트워크에 하나 이상의 라우터가 존재할 경우 더 나은 경로로 보내기 위해 호스트에게 패킷의 경로를 바꾸게 하는 패킷

된다. 즉 자동구성(Auto Configuration) 기능이 제공되며, 자동구성 방식엔 Stateless방식과 Stateful 방식이 있다[3,4].

2.3.1 Stateless 방식의 자동설정

Stateless 방식이란 RA 메시지를 이용하여 라우터로부터 Prefix 주소정보를 수신 받고, 자신의 인터페이스 ID를 이용하여 IP를 설정하는 방식으로서, 다음과 같이 자동으로 설정된다.

① Link local 주소 생성: Link local Prefix인 "fe80::/64"와 자신의 인터페이스 ID(MAC 주소)를 조합하여 Link local 주소 생성

② RS 메시지 송신: All Router Multicast Address로 라우터 요청 메시지를 송신하여 라우터 통신 메시지를 요구

③ RA 메시지 수신: 라우터 통지 메시지 내에 있는 해당 Network Prefix 정보를 획득

④ IP 주소 생성: Network Prefix와 자신의 인터페이스 ID를 이용하여 IPv6 주소 생성

2.3.2 Stateful 방식의 자동설정

Stateful 방식에서는 특정 서버가 IP 주소를 관리한다. IPv4에서도 사용된 자동구성방식으로 IPv6에서는 DHCPv6(IPv6 for Dynamic Host Configuration Protocol) 서버가 필요하다. 또 DHCPv6는 네트워크 Prefix부 뿐만 아니라 Host부에 해당하는 인터페이스부까지 DHCPv6가 일괄적으로 관리하도록 되어있다.

2.4 DAD(Duplicate Address Detection)

IPv6에서 IP를 구성하는 방법(stateless, stateful) 2가지 중 어느 방법으로 IP를 설정하더라도 DAD과정을 거쳐서 해당 IP가 이미 사용 중인지 아닌지 확인하게 된다.

DAD의 동작을 설명하면, 먼저 호스트가 자동으로 구성한 새로운 IP가 포함된 NS 메시지를 로컬 네트워크에 전송한다. NS 메시지를 수신한 네트워크 내의 호스트들은 자신의 IP와 비교하여 동일하다면 NS 메시지를 보낸 호스트에게 NA 메시지를 보내고, 다르면 Neighbor Cache를 업데이트 한다. NA 메시지를 수신한 호스트는 해당 IP가 이미 사용 중이라서 자신이 사용할 수 없는 주소라고 판단한다. 따라서 네트워크에 접속할 수 없게 된다.

DAD를 수행하기 위해서 표 3과 같은 항목의 값이 필요하며, 이 값은 시스템 관리자가 설정할 수 있다[4].

그림 2는 동일한 IP가 없는 경우 자동 주소 설정 절차를 보인다. 설정된 DupAddrDetectTransmits 값만큼 NS패킷 전송 후 RetransTimer 시간만큼 대기한다. 마지막 RetransTimer 시간이 지나도록 NA 응답이 없을 경우 인터페이스에 새로 구성한 IP를 할당하고 통신을 시작한다.

표 3. DAD 수행에 필요한 내용

항 목	설 명
DupAddrDetect Transmits	DAD 과정이 수행되는 동안 전송하는 연속된 NS 메시지의 개수. 0이면 DAD 과정을 수행하지 않고, 1이면 재전송 없이 한 번만 전송한다. 기본값은 1이며 이 값은 링크타입에 따라 값이 달라진다.
RetransTimer	DupAddr DetectTransmits가 1보다 큰 경우, DAD과정 수행 시 호스트가 NS 메시지를 재전송하는 시간 간격.

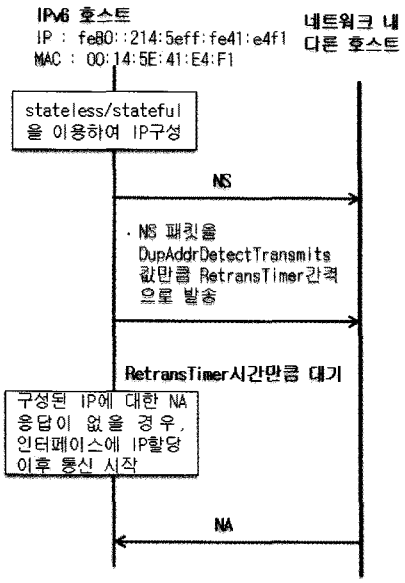

그림 2. 중복 IP가 없을 때 자동주소설정

그림 3은 특정 호스트가 이미 사용 중인 IP를 자동 설정하려고 하는 경우 주소 설정에 실패하는 과정을 나타낸다. 호스트 A가 먼저 fe80::214:5eff:fe41:e4f1 IP를 사용 중인 상황에서 호스트 B가 동일한 IP를 사용하려고 시도할 경우, 호스트 A는 NA 패킷을 호스트 B로 보내어 이미 사용 중인 IP임을 알린다. 그래서 호스트 B는 자동 설정하려는 IP를 사용하지 못하므로 네트워크에 접속할 수 없게 된다.

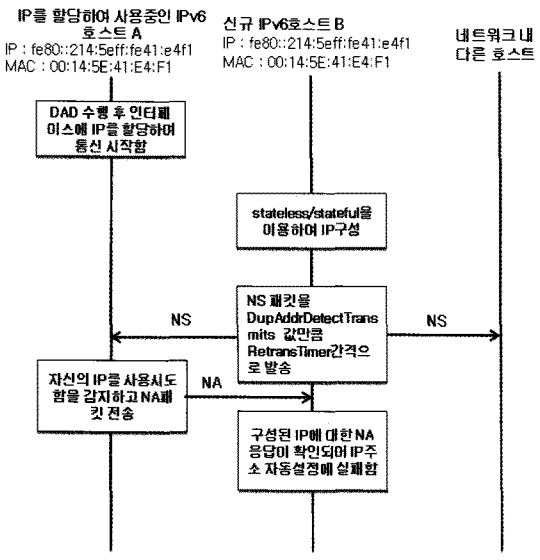

그림 3. 이미 사용 중인 IP를 자동 설정한 경우

3. 호스트 탐색 및 네트워크 접속 차단을 위한 에이전트 시스템

3.1 에이전트 시스템의 동작 구조

그림 4는 에이전트 시스템의 동작 구조를 나타내고 표 4는 본 실험에서 사용한 설정 파일의 구성을 보인다. 여기서 패킷 캡쳐 시 ICMPv6 프로토콜이면서 이더넷 근원지 주소가 에이전트의 MAC 주소가 아닐 경우에만 패킷을 캡쳐하도록 필터를 설정한다. 그 이유는 에이전트가 발생시킨 ICMPv6 패킷까지 차단 및 격리하게 되면 에이전트 자체가 통신할 수 없는 상태에 놓이게 되기 때문이다.

3.2 각 스레드의 기능

본 에이전트 시스템에서 구현한 주요 스레드로는 Monitoring Thread, Blocker Thread, Update Thread, Search Thread 등이 있다.

Monitoring Thread는 캡쳐를 통해 ICMPv6 패킷을 획득하는 스레드로서 획득한 패킷 중 NDP를 구분하여 BlockerQueue와 UpdateQueue에 저장한다. 이때, 두 개의 큐에 저장되는 패킷은 동일하며 추가로 NDP의 종류를 포함한다.

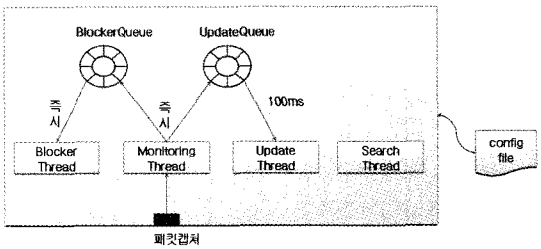

그림 4. 에이전트 시스템의 동작 구조

표 4. 설정 파일(config file)의 구성

설정 내용	설 명
DEVICE_NAME eth0	모니터링 및 차단 시 사용할 어댑터
SEARCH_IP6 fe80::2946:7936:8fde:41f1	탐색할 IPv6 주소
SEARCH_INTERVAL 2	탐색주기(단위:초)
BLOCK_IP6 fe80::2946:7936:8fde:41f1	차단할 IPv6 주소
BLOCK_MAC 11:0C:29:21:3C:78	차단할 MAC 주소

Blocker Thread는 Monitoring Thread에서 캡처한 ND(Neighbor Discovery) 패킷을 분석하여 차단 IP 또는 MAC이라면 패킷의 종류에 따라 멀티캐스트(multicast)[7-9] 또는 유니캐스트(unicast) IP로 변조된 NA를 전송하여 차단을 수행하는 스레드이다.

Update Thread는 Monitoring Thread에서 캡처한 ND 패킷을 이용하여 IP, MAC정보를 획득하는 스레드이다. 캡처한 패킷이 RA라면 IP, MAC 이외에 라우터의 정보도 획득한다.

Search Thread는 탐색 또는 차단을 위해, 설정한 IP가 사용되고 있는지 주기적으로 탐색을 요청하는 스레드이다.

3.3 특정 호스트 탐색

3.3.1 호스트 탐색 패킷 구조

탐색하고자 하는 IP를 ICMPv6 target address필드에 설정한 NS를 link local all node IP(ff02::1)로 전송하여 정보를 요청한다.

3.3.2 호스트 탐색 동작

NDP의 NS와 NA 메시지를 이용하여 네트워크에 존재하는 호스트를 탐색한다. 그림 5에서 에이전트가 NDP를 이용해 호스트를 탐색하는 동작을 설명한다.

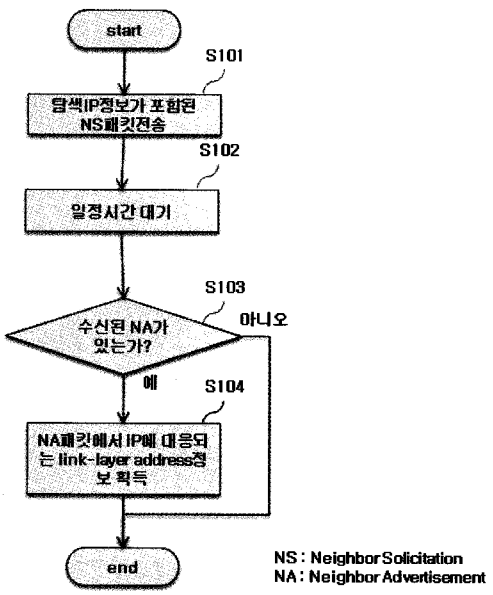

그림 5. 특정 호스트 탐색

탐색하고자 하는 IP가 속한 multicast IP를 목적지 IP로 설정하여 multicast 영역 내에 존재하는 모든 호스트에게 NS 패킷을 전송해서 탐색IP의 정보를 요청한다. 패킷 전송 후 호스트의 처리속도 및 네트워크 전송 속도를 고려하여 일정시간 대기한다. 일정시간 대기 후 탐색 대상인 호스트가 보내온 NA를 수신하면 해당 패킷에서 링크계층 주소 정보(이더넷이면 MAC주소)를 획득한다. 이렇게 획득한 정보를 탐색 리스트에 추가하거나 갱신한다.

3.4 특정 호스트에 대한 네트워크 접속 차단

3.4.1 특정 호스트 차단용 패킷 구조

호스트 차단을 위해 에이전트 시스템은, 기본적으로 차단 대상 호스트가 사용하는 IP에 대해서 link local에 존재하지 않는 가상의 MAC 주소가 설정된 NA(Neighbor Advertisement)를 link local all node multicast IP로 전송한다. 이 패킷을 수신한 네트워크 내 호스트들은 에이전트가 조작해 보낸 NA를 이용하여 neighbor cache를 업데이트하므로 결과적으로 차단 대상 호스트와는 통신이 되지 않게 된다. 본 패킷은 에이전트 시스템에서 조립되는 것으로서 특정 호스트를 차단하기 위한 NA 패킷 중 주요 내용은 표 5와 같다.

3.4.2 네트워크 접속차단 방법

악의적인 특정 호스트가 네트워크에 접속할 수 없도록 NDP의 동작 중 DAD 동작을 이용하여 구현한다. 네트워크에서 확인되는 NDP 패킷의 송신지 링크계층주소를 조사한 결과 네트워크 접속을 차단해야 할 필요가 있다면, 가상의 링크계층주소를 설정하여 송신지의 링크계층주소로 NA 메시지를 전송한다. 차단 대상 호스트가 NA 메시지를 수신하면 이 호스트는 DAD 동작의 결과로서 이미 사용되고 있는 IP라고 판단하게 된다.

특정 호스트를 접속 차단하기 위한 정책 설정 시 설정정보는 차단 대상 IP 또는 차단 대상 링크계층주소가 설정되며 두 항목 모두 다 설정될 수도 있다. 또 추가적으로 정책의 시작시간, 종료시간을 포함할 수 있다.

그림 6은 에이전트가 ND 패킷을 캡쳐 했을 때의 동작을 설명한다. 여기서, 근원지 정보는 이더넷 헤더의 근원지 링크 계층 주소(link layer address) 또

표 5. 특정 호스트 차단을 위한 NA 패킷 구조

헤 더	필 드	크기(bit)	설정 값	설 명
이더넷	destination address	48	33:33:00:00:00:01 (ipv6 neighbor discovery link-local all node multicast)	목적지MAC
	source address	48	[에이전트 MAC]	근원지MAC
	packet type ID	16	0x86dd(ipv6)	타입
ipv6	version	4	0x60	프로토콜 버전
	traffic class	8	0	QoS
	flow label	20	0	QoS
	payload length	16	0x20(32)	상위 프로토콜 데이터길이
	next header	8	0x3a(icmp6)	다음 헤더 타입
	hop limit	8	0xff(255)	ipv4 ttl과 동일
	source address	128	[차단대상호스트 IP]	근원지 IP
	destination address	128	ff02::1 (link-local all node multicast)	목적지 IP
icmpv6	type	8	136(NA)	타입
	code	8	0	세부 타입
	checksum	16	[패킷 별 계산]	패킷유효성 검사
	reserved	32	0	예약
	target address	128	[차단대상호스트 IP]	요청 대상 ip
	type	8	0x02(target link-layer address)	option type
	length	8	0x01	option length
	target link layer address	48	00:c0:26:90:8f:e8 (조작된 MAC)	option data

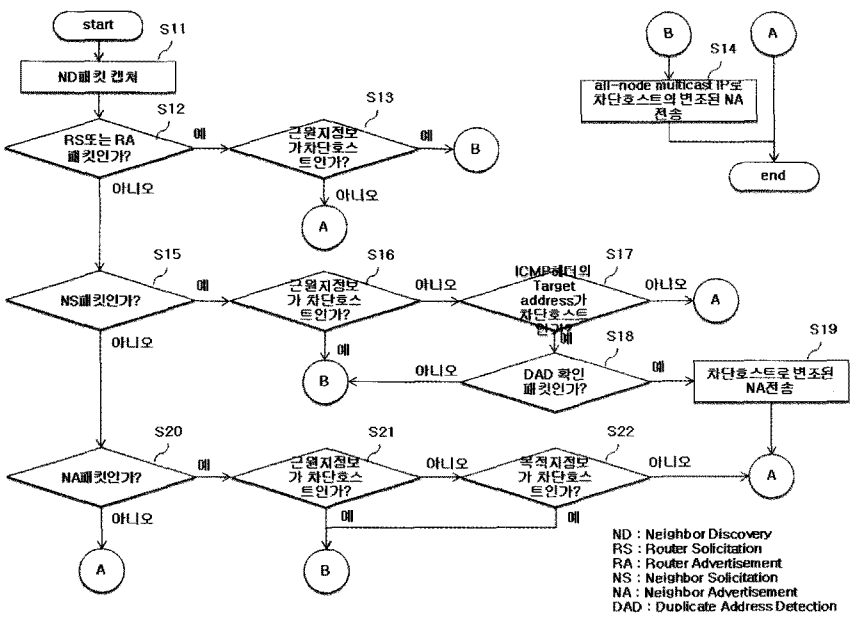

그림 6. 특정 호스트에 대한 네트워크 접속 차단

는 IP 헤더의 근원지 주소가 되며, 목적지 정보는 ICMP 헤더의 Target address 또는 Target link layer address이다. 그리고 차단 대상 호스트를 구분하는 방법은 IP와 링크 계층 주소 정보를 기초로 한다.

그림 6에서 보는 바와 같이 ND 패킷이 캡쳐되면(단계 S11), 패킷이 RS 또는 RA인지 판단한다(단계 S12). 판정결과 RS 또는 RA패킷이라면 근원지 정보가 차단대상 호스트인지 판정한다(단계 S13). 차단대상 설정 파일에 존재하는 것으로 판정되면 all node multicast IP로 차단대상 호스트의 MAC 주소를 변조한 NA패킷을 멀티캐스트 IP로 전송하고(단계 S14), 존재하지 않는다면 처리를 종료한다.

단계 S12에서 RS또는 RA패킷이 아니라면, NS패킷인지 조사한다(단계 S15). 판정결과 NS패킷이라면, 근원지정보가 차단 대상 호스트인지 판단한다(단계 S16). 차단대상 호스트라면 단계 S14를 수행한 후 처리를 종료하고. 차단대상 호스트가 아니라면 ICMP 헤더의 Target address가 차단대상 호스트인지 판단한다(단계 S17). 차단대상 호스트로 판정되면, DAD 패킷인지 조사하고(단계 S18), DAD 패킷이라면 차단대상 호스트에게 변조된 NA 패킷을 전송하여 차단대상 호스트를 차단한 후(단계 S19), 처리를 종료한다. 그리고 DAD 패킷이 아니라면 단계 S14를 수행한 후 처리를 종료한다. 한편, 단계 S17에서 ICMP 헤더의 Target address가 차단대상 호스트가 아니라면 처리를 종료한다.

단계 S15에서 NS 패킷이 아니라면, NA 패킷인지 판단한다(단계 S20). 판단 결과 NA 패킷이라면 근원지정보가 차단 대상 호스트인지 판단하고(단계 S21), 차단대상 호스트라고 판정되면, 단계 S14를 수행한 후 처리를 종료한다. 차단대상 호스트가 아닌 것으로 판정되면 목적지정보가 차단대상 호스트인지 조사한다(단계 S22). 목적지정보가 차단대상 호스트로 판단되면 마찬가지로 단계 S14를 수행한 후 처리를 종료하고, 목적지정보가 차단대상 호스트가 아닌 것으로 판단되면 처리를 종료한다.

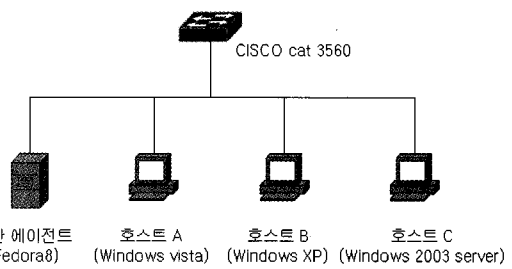

그림 7. 시험망의 구성

4. 구현결과

본 에이전트 시스템은 fedora8 운영체제, C++언어, g++ v4.1.2 컴파일러, libpcap 1.0.0 라이브러리를 사용하여 구현하였다.

4.1 시험망 구성

본 논문에서 구현한 특정 호스트 탐색 및 네트워크 접속 차단을 위한 에이전트 시스템을 검증하기 위해 그림 7과 같은 시험망을 구축하였다.

cisco cat3560은 IPv6와 IPv4가 동시에 지원하는 스위치이다. 기본적으로 생성되는 link local IP 외에 fec0:10:: 네트워크 주소의 site local 주소를 추가로 생성할 수 있다. 여기에 고정 IP를 설정한다면, 호스트에 link local, site local, 고정 IP 등 3개의 IP를 설정할 수 있게 된다.

구현한 에이전트 시스템의 기능을 확인하기 위해, 앞에서 설명한 표 4와 같은 호스트 차단 정책을 설정하고, 차단 대상 호스트에서 multicast IP(ff02::1)로 ping을 시도했다. ping 테스트 결과와 시도 횟수에 따른 IP 설정 상태를 조사하였다.

4.2 호스트 탐색 시험 결과

그림 7과 같은 시험망에서, 각 호스트에 자동 설정된 IP에 대응하는 MAC주소를 요청하고, 수신된 NA를 이용하여 MAC주소를 획득한 결과를 표 6에 나타내었다.

4.3 호스트 차단 시험 결과

차단 대상 호스트에서 multicast IP(ff02::1)로 ping 테스트를 수행하였다. 호스트 차단 정책 설정 즉시 에이전트 시스템은 차단 대상 호스트에게 변조된 NA 패킷을 전송함을 확인하였다. 각 호스트에 설정되는 IP는 link local IP, site local IP, 고정 IP로 차단을 수행하는 시점에서 에이전트는 차단 대상장비의 IP를 모두 설정파일에 저장하고 있어 사전에 알고 있다는 전제 하에 테스트를 수행했다.

ping테스트 결과와 IP 설정 상태를 조사한 결과를 표 7에 나타내었다.

대부분의 상황에서 정상적으로 차단이 수행되는 것을 확인하였으나, 고정 IP를 설정한 경우 통신이 정상적으로 되는 문제가 발생하였다. 이 문제를 확인하기 위해 캡쳐한 패킷을 분석한 결과 ping 테스트 시 사용한 ff02::1 multicast IP가 루프백 인터페이스에 등록되어 있어 실제로 패킷이 외부로 전송되는 것이 아니고 루프백 됨을 확인하였다. 그래서 multicast IP를 사용하지 않고 특정 호스트의 IP로 테스트한 결과 정상적으로 차단됨을 확인하였다.

에이전트 시스템의 동작을 테스트한 결과, 차단 수행 후 3개의 장비에서 설정된 IP에 대해서 설정이 해제되는 것을 확인하였다. 그러나 예외적으로 Windows vista의 경우 IP설정이 해제된 후, link local IP와 site local IP를 변경해서 네트워크에 접속하는 것을 확인하였다. 실제 본 에이전트 시스템을 이용하여 특정 호스트를 접속 차단하려고 할 때는 MAC주소로 차단 대상 호스트를 결정해야 함을 알 수 있다.

5. 결 론

본 논문에서는 IPv6 환경에서 특정 호스트를 탐색하고 부적격 사용자의 네트워크 접속을 차단할 수 있는 에이전트 시스템을 구현하였다. 본 시스템의 기능을 검증하기 위해 IPv6를 지원하는 스위치와 윈도우 계열 운영체제를 탑재한 호스트로 시험망을 구축하고, 테스트를 실시하였다.

특정 호스트를 탐색하기 위해 시험한 결과, 각 호스트에 자동 설정된 IP에 대해 MAC 주소를 요청하고, 수신된 NA를 이용하여 MAC 주소를 획득할 수 있었다. 또 특정 호스트에 대해 네트워크 접속차단을 시험하였다. 차단 대상 호스트에서 multicast IP (ff02::1)로 ping 테스트를 수행하면, 에이전트 시스템은 차단 대상 호스트에게 변조된 NA 패킷을 전송함을 확인하였다. 따라서 차단대상 호스트는 자신의 IP 주소가 이미 사용 중인 것으로 알고 네트워크에 접속하지 못함을 확인하였다.

대부분의 상황에서 정상적으로 차단이 수행되는 것을 확인하였으나, 고정 IP를 설정한 경우 통신이 정상적으로 되는 문제가 발생하였다. 이 문제를 확인하기 위해 캡쳐한 패킷을 분석한 결과 ping테스트 시 사용한 ff02::1 multicast IP가 루프백 인터페이스에 등록되어 있어 실제로 패킷이 외부로 전송되는 것이 아니고 루프백 됨을 확인하였다. 그래서 multicast IP를 사용하지 않고 특정 호스트의 IP로 테스트한 결과 정상적으로 차단됨을 확인하였다.

예외적으로 Windows vista의 경우 자동 설정한 IP를 해제한 후, link local IP와 site local IP를 변경해서 네트워크에 접속하는 것을 확인하였다. 따라서 실제 본 에이전트 시스템을 이용하여 특정 호스트를 접속 차단하려고 할 때는 MAC 주소로 차단 대상 호스트를 결정해야 함을 알 수 있다.

향후 과제로는, IPv6망 탐색 및 차단을 테스트하

표 6. 호스트 탐색결과

OS	IPv6	탐색여부
Windows XP	fec0:10::21f:c6ff:fe8b:2a2c/64	NA수신, MAC획득
Windows Vista	fec0:10::161:8888:95f9:be19/64	NA수신, MAC획득
Windows 2003 Server	fec0:10::211:25ff:fe22:a29d/64	NA수신, MAC획득
switch	fec0:10::10/64	NA수신, MAC획득

표 7. 호스트 차단 시험결과

장비명	Ping 테스트		차단대상 호스트의 IP 설정 정보	
	차단 전	차단 후	차단 전	차단 후
호스트 A (vista)	정상	에러 발생[1]	link local IP 설정 site local IP 설정 고정IP설정	link local IP변경됨 site local IP변경됨 고정IP설정 해제
호스트 B (xp)	정상	에러 발생[2]	link local IP 설정 site local IP 설정 고정IP설정	모든 IP설정 해제
호스트 C (2003 server)	정상	에러 발생[2]	link local IP 설정 site local IP 설정 고정IP설정	모든 IP설정 해제

주) 1) 지정한 네트워크 이름의 형식이 올바르지 않습니다.
2) Invalid source route specified

기 위해, 본 논문에서 테스트한 3가지 윈도우 계열 이 외에 IPv6를 지원하는 Windows 7, Windows 2008 server, Linux, MacOS에 대해서도 테스트할 계획이다. 또 시스코 스위치 이외의 다양한 스위치에서도 본 에이전트 시스템의 동작을 시험할 필요가 있다.

참 고 문 헌

[1] 오하영, 채기준, 방효찬, 나중찬, "IPv6 네트워크 환경에서 MCGA를 고려한 통합적인 보안관리 방안," 정보처리학회 논문지 C, 제14-C권, 제1호, 2007.

[2] 한국인터넷진흥원, http://www.vsix.kr/jsp/intro/intro_01.jsp

[3] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," *IETF RFC 2460,* Dec. 1998.

[4] S. Thomson and T. Narten, "IPv6 Stateless Address Auto-Configuration," *IETF RFC 2462,* Dec. 1998.

[5] A. Conta and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," *IETF RFC 2463,* Dec. 1998.

[6] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," *IETF RFC 2461,* Dec. 1998.

[7] M. Crawford, "Transmission of IPv6 Packets over Ethernet Networks," *IETF RFC 2464,* Dec. 1998.

[8] S. Deering, W. Fenner, and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6," *IETF RFC 2710,* Oct. 1999.

[9] 성수련, 김기영, 신용태, "이동 IPv6 환경에서 지역성에 기반한 효율적인 멀티캐스트 전송 메카니즘," 정보처리학회논문지 C, 제12-C권, 제3호, 2005.

정 연 기

1996년 영남대학교대학원 정보통신 전공(공학박사)
1985년~1990년 가톨릭상지대학 전산정보처리과 조교수
1998년 호주 뉴캐슬대학교 컴퓨터공학과 방문교수
1990년~현재 경일대학교 컴퓨터공학부 교수
관심분야 : 네트워크 관리, 센서 네트워크, 멀티미디어 통신, LAN/WAN 설계

문 해 은

2000년 2월 영남대학교 전자공학과 졸업
2002년 2월 영남대학교 정보통신공학과 졸업(공학석사)
2002년 3월~현재 (주)넷맨 수석연구원/연구소장
관심분야 : 네트워크 관리, 네트워크 보안, MPLS/VPN, TMN, TINA