무선 액세스 포인트 기반의 NAPT 기능 설계 및 구현

이승호[U], 송병훈, 정광수, 오승준
광운대학교 전자공학부 컴퓨터통신연구실
[U]shlee@adams.gwu.ac.kr, byungh@ccl.gwu.ac.kr,
kchung@daisy.gwu.ac.kr, sjoh@daisy.gwu.ac.kr

Design and Implementation of NAPT Function Based on Wireless Access Point

Seungho Lee[U], Byunghun Song, Kwangsue Chung, Seoungjun Oh
School of Electronics Engineering, Kwangwoon Univ.

요 약

최근 다양한 무선 인터넷 기술 중에서도 무선랜을 이용한 서비스는 기존의 유선랜 기반의 서비스들을 그대로 적용 할 수 있다는 큰 장점 때문에 상당한 관심이 집중되고 있다. 무선랜 기술의 핵심 중 하나는 기능적으로 유무선의 호스트들 간의 서비스 연동을 담당하는 장비인 무선 액세스 포인트에 있다. 현재 국내외에서 상용화된 대부분의 액세스 포인트 장비는 단순한 브리지 및 게이트웨이 기능과 인터넷 주소의 부족에 의한 해결책으로 기본적인 NAT(Network Address Translation) 기능만을 지원한다. 그러므로 다양한 응용에 따른 서비스의 연동을 가능하게 하는 기술에 대한 지원이 미비하다 할수 있다. 사설망과 공인망 사이의 서비스 연동을 NAT 기반의 네트워크에서 동작하도록 하기 위한 연구가 바로 PAT(Port Address Translation) 기술이다. 본 논문에서는 기존의 NAT 기반의 모듈들과 효과적으로 연동할 수 있는 최적화된 PAT 기능을 설계 및 구현하였다. 그리고 이를 통합한 NAPT 액세스 포인트를 개발하여 그 기능을 시험하고 검증하였다.

1. 서론

최근 무선 인터넷 기술의 급속한 발전으로 말미암아 인터넷 사용자의 폭발적인 증가와 다양한 인터넷 응용 서비스의 출현이 중요한 이슈로 등장하고 있다. 그중 무선랜을 이용한 서비스는 기존의 유선랜에 비해 전송속도가 다소 느린 단점에도 불구하고 무선으로서 가지는 이동성, 확장성, 망 구성의 용이성 등의 이점과 유선랜 기반의 서비스들을 그대로 적용할 수 있다는 큰 장점 때문에 상당한 관심이 집중되고 있다 [1].

무선랜 기술에 있어 유무선 호스트들 간의 서비스 연동을 담당하는 무선 액세스 포인트는 핵심적인 기술요소라 할수 있다. 초기의 액세스 포인트 장비는 기본적으로 브리지 및 게이트웨이 기능만을 수행하였다. 그러나 인터넷 사용자의 폭발적인 증가로 인한 인터넷 주소부족 문제가 대두되면서 NAT(Network Address Translation)와 같은 주소문제 해결 방안을 지원하는 제품들이 많이 개발되어지고 있다.

NAT는 사설망 내부의 사설 IP주소를 공인 IP주소로 변환함으로써 사설망 내부의 호스트가 인터넷으로의 접근을 가능하게 해주는 기술이다[2]. 이때, 공인 IP주소는 1:1 혹은 N:1의 비율로 공유됨으로써 인터넷 주소부족 문제에 대한 단기적인 해결책이 될 수 있으나 외부망으로부터의 서비스 요청을 처리하는 데에는 많은 제약이 따른다. 이러한 이유 때문에 외부망에 대한 서비스를 NAT망의 내부의 호스트와 연동 할 수 있게 하는 기술인 PAT(Port Address Translation)에 대한 연구가 활발히 진행 중에 있다.

본 논문에서는 기본적인 NAT기능 외에도 응용들의 포트주소를 변환하여 서비스 연동을 해주는 PAT기술과 이를 통합한 NAPT(Network Address Port Translation) 지원 액세스 포인트를 임베디드 플랫폼 상에 설계 및 구현하였다. 구현한 액세스 포인트를 사용하여 구성된 무선랜 기반의 사설망 내에서 FTP, H.323, X-terminal 등의 여러 가지 서비스를 외부망과 성공적으로 연동하였을 뿐만 아니라, 반대로 외부의 사용자에게도 투명한 서비스를 제공 할수 있었다.

본 논문의 2장에서는 무선랜 기술 및 주소변환 기술에 관해 기술하였고, 3장에서는 NAPT 기능의 설계 및 구현에 대해 기술하였다. 4장에서는 액세스 포인트의 기능을 시험하기 위한 시험 망의 구성과 동작 시험 결과에 대해 기술하였고 끝으로 5장에서 결론을 맺었다.

2. 관련 연구

2.1 무선랜과 액세스 포인트

무선랜 기술은 1997년 2Mbps의 대역으로 상용화가 시작되어 현재 최대 11Mbps, 2.4GHz(IEEE 802.11b)의 전송속도를 가지는 제품들이 주로 상용화되고 있으며, 최근에는 최대 54Mbps, 5GHz(IEEE 802.11a)의 기술이 상용화를 눈앞에 두고 있다.

무선랜은 유선랜을 대체하기보다는 기간망과 사용자간의 수십 미터 이내의 무선구간에 종단 연결점을 제공한다는 개념으로 구성되며, 크게 애드혹(ad-hoc) 방식과 인프라스트럭처 방식으로 망을 구성할 수 있다[3]. 애드혹방식으로 구성하는 경우 무선랜상의 하나의 호스트는 서버가 되면서 동시에 클라이언트가 되는 P2P(peer-to-peer) 방식으로 동작한다. 인프라스트럭처 방식에서는 클라이언트-서버 방식으로 동작하여 망 내부의 호스트들은 액세스 포인트를 통해 상호간의 통신이나 망 외부로의 접근이 가능하게 된다. 인프라스트럭처 방식의 무선망 내에서 액세스 포인트는 기본적으로 브리징을

통해 호스트 상호간 혹은 호스트와 유선망간을 MAC 레벨로 연결해 주는 기능을 수행한다. 최근에는 네트워크레벨의 라우팅기능 뿐만이 아니라, DHCP, SNMP, NAT, PPP 접속 지원 등의 고급 서비스까지도 담당하는 추세로 발전하고 있다.

2.2 사설망에서의 주소변환 기술

사설망에서의 주소변환 기술의 목적은 사설망에 위치하여 사설 IP 주소를 사용하는 호스트가 공인망에 위치한 타 네트워크를 이용할 수 있도록 사설 IP 주소를 적절한 공인 IP 주소로 변환해 주는 것이다. 이를 위해, 주소변환기술은 기본적으로 OSI 모델의 네트워크 계층에서 구현되며, 사설 IP 주소와 대응되는 공인 IP 주소를 매핑하기 위한 NAT 라우팅 테이블을 이용한다. 그림 1은 일반적인 NAT 서비스를 도시한 것이다.

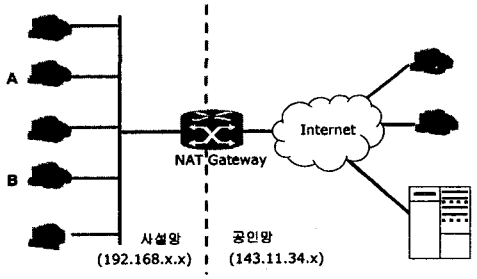

그림 1. NAT 서비스

주소변환 기술을 기능별로 세분화하면 basic NAT와 NAPT, RSIP(Realm Specific IP) 등으로 구분 지을수 있다 [5].

㉠ Basic NAT는 그림 1과 같이 사설망과 공인망의 경계에 존재하는 라우터에서 동작하며 네트워크 계층의 주소 변환을 수행한다. 주소변환이 네트워크 계층에서 일어나므로 변환 속도가 빠르고, 구현이 비교적 간단하다. 그림 1에서 사설망의 호스트 A에서 공인망의 호스트 X로 접근하는 경우 데이터 플로우에 하나의 공인 IP(globalIP_1)가 할당되어 통신한다. 이 때, NAT 테이블에는 (localIP_A, globalIP_1)로 기록해 놓는다. 사용 가능한 공인 IP가 하나만 존재할 경우 Basic NAT는 사설 IP와 공인 IP를 1:1로 바인딩한다.

㉡ NAPT는 전송계층의 포트변환을 이용한 N:1 바인딩을 지원한다[4]. 즉 Basic NAT에 PAT기능을 추가하여 사용가능한 IP가 하나일 때도 포트변환을 통한 여러 호스트간 IP 공유를 가능하게 해준다. NAPT는 Basic NAT에서와 유사하게 NAT 테이블을 관리하게 되는데, 변환되는 포트에 대한 매핑정보가 추가된다. 예를 들어 그림 1에서 호스트 A, B가 동시에 하나의 공인 IP를 이용해 데이터를 전송하고자 할 경우 NAT 테이블은 표 1과 같은 형태로 기록된다.

NAPT에서는 주소변환을 위해 네트워크 계층의 목적지 주소 정보뿐만 아니라 전송계층의 포트번호로 플로우를 구별하므로 처리가 복잡하고 속도가 느린 단점이 있지만, Basic NAT 기법의 단점을 극복하여 IP 재사용 효율을 극대화 시켰으며 현재 가장 많이 사용되고 있는 기법이다.

표 1. NAT 테이블

사설망 내부 IP	공인망 IP
localIP_A : Port_A	globalIP_1 : Port_xx
localIP_B : Port_B	globalIP_1 : Port_yy

㉢ RSIP는 터널을 이용한 새로운 주소 변환방식이다. 구조적으로 클라이언트/서버 구조를 가지며, 서버는 클라이언트에서 사용할 IP주소 변환에 필요한 파라미터(IP주소, 포트번호, 사용시간 등)와 터널링을 협상하며 각 클라이언트에 관한 상태정보를 관리한다.

3. NAPT 기능의 설계 및 구현

그림 2는 임베디드 환경을 고려하여 설계한 NAPT 액세스 포인트에서 사용되는 통신 프로토콜의 구조를 나타낸다. 구현된 NAPT 모듈은 크게 NAT와 PAT기능으로 구분되어 진다.

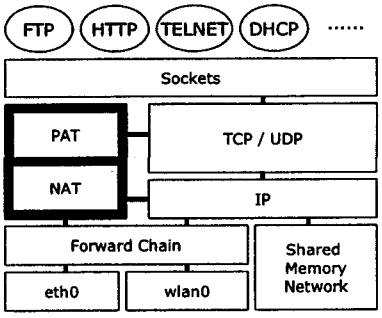

그림 2. PAT 액세스 포인트의 프로토콜 스택

본 논문에서도 사용하였지만 최근 각광받고 있는 임베디드 운영체제인 임베디드 리눅스에서 기본적으로 제공하는 basic NAT 기법으로는 IP Masquerading이 있는데 2.2.x 커널에서는 ipchains의 일부분으로 구현되어 있다. 그림 2의 NAT에 해당하는 부분이 실제로 IP Masquerading 부분이며, 본 논문에서는 여기에 동적인 포워딩 정책결정을 위한 PAT Agent를 구현하였다. 특히, PAT Agent와 관리자간의 인터페이스를 웹을 이용한 GUI로 구현함으로써 NAPT를 제어하는데 편의를 제공하였다. 기존의 PAT 기능은 빈번한 포트포워딩 정책을 시스템 관리자 권한으로 복잡하게 설정해야하는 문제점이 있었다.

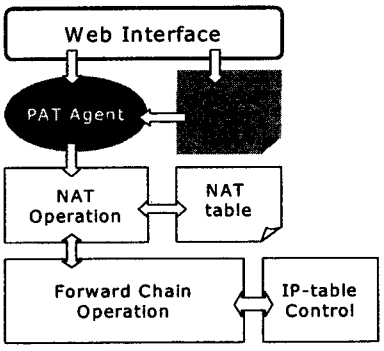

그림 3 구현한 NAPT 구성도

그림 3은 액세스 포인트에서 NAPT기능을 지원하기 위해 구현한 PAT Agent의 동작과정을 보이고 있다. 웹 인터페이스를 통해 전송 프로토콜, 사설망 내의 서버 IP와 서비스할 포트번호, 외부로부터 요청되는 포트번호로 구성된 메타파일이 생성된다. 이후 사용자 명령에 의해 PAT Agent는 메타파일을 참조하여 포워딩 및 서비스 정책을 갱신한다. 이때 특정 응용들(예 : FTP)은 주소 변환 과정에서 간단한 IP 헤더변환

외에 페이로드 부분을 수정해야 하므로 미리 구성된 특별한 ALG(Application Level Gateway) 모듈을 필요로 한다.

4. 시험망의 구성 및 동작 시험

액세스 포인트의 구현을 위해 사용한 플랫폼은 EP860P CLLF 보드이다. EP860P CLLF는 10/100M Ethernet 포트와 PCMCIA 슬롯을 통해 유/무선 네트워킹을 지원한다. 또한 구현에 사용한 임베디드 운영체제는 HardHat Linux (kernel 2.2.14)이며, 액세스 포인트 프로토콜 스택은 모두 리눅스기반으로 구현하였다.

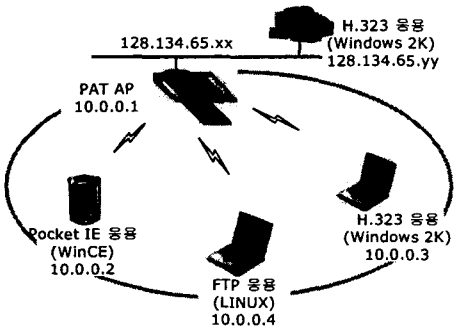

그림 4. PAT AP를 이용한 사설망 구축

NAPT 액세스 포인트를 시험하기 위해 구성한 망은 그림 4와 같으며, 무선랜 기반의 사설망 내에서는 FTP 서버와 대표적인 H.323 응용인 넷미팅을 사용하였다. 또한 PDA와 같은 이동단말에서의 인터넷 연결을 확인하기 위해서 pocket IE(Internet Explorer)를 사용하였다.

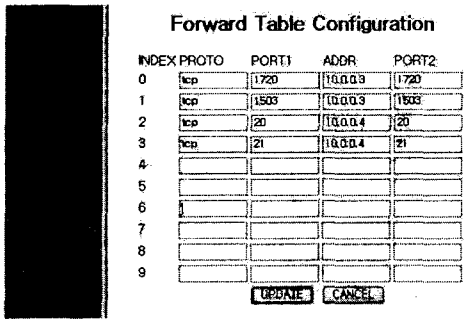

그림 5. PAT 설정 인터페이스

그림 5는 웹을 통한 PAT 정책의 설정 과정이다. PAT 정책은 응용의 특성과 연결에 따라 빈번하게 설정해야 할 필요가 있다. 그러므로 손쉬운 정책설정 인터페이스가 필요하다.

PROTO과 PORT1은 처리할 서비스의 프로토콜과 포트번호를 설정하는 부분이며 ADDR과 PORT2는 요청된 서비스를 처리할 사설망내 호스트의 IP주소와 전달할 포트번호이다. 본 논문에서는 시험을 위해서 편의상 동일한 포트번호를 전달하도록 설정하였다. 예를 들어 외부망(128.134.65.0 네트워크)으로부터 FTP요청을 들어오게 되면 설정된 테이블 내용중 PORT1을 검색하여 사설망내에 서비스할 호스트가 존재하는지 판별한다. 존재한다면 그 호스트의 IP를 확인하고 PORT1을 PORT2의 포트번호로 변환하여 요청을 전달한다. 이에 대한 응답은 다시 액세스 포인트로 전달되어 IP주소와 포트번호 변환과정을 거친 다음 공인망 상의 클라이언트로 전달된다. 이러한 정책을 기반으로 시험한 FTP, H.323, pocket IE 응용들은 모두 사설망과 공인망 사이에서 성공적으로 연동됨을 확인 할수 있었다.

그림 6은 개발한 액세스 포인트를 지나는 트래픽들의 정책을 나타낸 것이다. ①에서는 변환되는 사설망주소(source)와 현재 통신하고 있는 공인망주소(destination), 그리고 포트의 변환이 나타나 있다. 실제로 변환 된 후의 주소는 사용가능한 공인망 IP가 유일하므로 생략되었다. ②에서는 사설망 내로 진입하는 서비스 요청에 대한 정책을 확인할 수 있다. 그림 5의 정책이 그대로 시스템에 적용되었음을 확인 할수 있다.

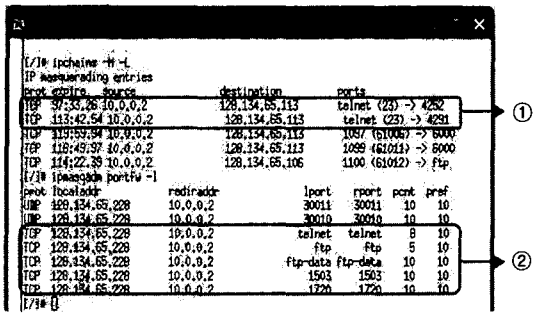

그림 6. NAT 및 PAT 테이블 확인

5. 결론

액세스 포인트는 무선랜 기술의 핵심적인 장비이며, 기본적으로 브리징과 게이트웨이 등이 주요기능이다. 여기에 최근 IP 주소부족 문제가 부각되면서 기존의 유선랜에서 사용되었던 주소변환기술을 적용한 액세스 포인트가 상용화되고 있으나 아직 외부망과의 서비스 연동차원에서는 부족한 점이 많았다.

본 논문에서는 IP공유를 위해 리눅스의 IP Masquerading을 이용하여 NAT 기능을 구현하였고 PAT기능을 위한 에이전트를 설계, 구현하여 이를 통합한 NAPT를 액세스 포인트 상에 구현함으로써 무선랜으로 구성된 사설망에서 다양한 서비스를 외부망에 제공할 수 있도록 하였다. 또한 본 논문에서 구현한 기능은 홈네트워킹이나 소호와 같은 소규모의 저렴한 네트워크를 구축하고 이를 기반으로 서비스를 제공하고자 하는 것이 주요 이슈로 대두되고 있는 현 추세로 볼 때 더욱 중요한 의미를 갖는다. 잘 알려진 것과 같이 리눅스를 기반으로 한 임베디드 시스템 상에 구현하여 비용면이나 차후 시스템 관리면에서도 많은 잇점이 있다.

향후 연구과제로는 PAT의 특성으로 인해 NAT기능만을 수행하는 액세스 포인트에 비해 부하가 많이 걸리는 문제를 보다 최적화 시키는 것에 대해 연구되어야 할 것이다.

참 고 문 헌

[1] 오민철, 송병훈, 정광수, "무선 환경에서의 사용자 인증을 지원하는 QoS제어 게이트웨이 구현," 한국정보과학회 춘계학술대회, pp 271-273, 2002.4

[2] K. Egevang, P. Francis, "The IP Network Adress Translator (NAT)", IETF RFC 1631, May 1994

[3] IEEE 802.11 Draft Standard 2.0, "Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifications," May 1995

[4] P. Srisuresh, K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", IETF RFC 3022, Jan. 2001

[5] 전우직, 이광희, "IP 주소 변환 기술에 관한 연구 동향," 정보통신연구원 간행물, 2000.1