2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

Plug&Play를 지원하는 이더넷 접속 장치의 설계 및 구현

°이상민, 윤영선, 은성배
한남대학교 정보통신공학과
e-mail:{smlee, ysyun, sbeun}@daniel.hannam.ac.kr

Design and Implementation of A Network Access Device Supporting Plug&Play

Sang-Min Lee, Young-Sun Yun, Seongbae Eun
Dept. of Information and Communication Eng., Hannam University

요약

여행자가 호텔에서나 회의실에서 인터넷에 접근하기 위하여 자신의 노트북을 이더넷 접속 포트에 연결할 때 이미 설정된 네트웍 파라미터를 변경하지 않고 Plug&Play 방식으로 접속할 수 있다면 매우 편리할 것이다. 기존의 DHCP, NAT 등의 프로토콜 등이 IP 주소가 설정되어 있지 않는 경우에 유용하나 설정된 주소 값을 변경없이 접근할 수 있도록 지원하지는 않는다. 본 논문에서는 Linux에서 지원하는 Masquerading 기능을 이용하여 Plug&Play 방식으로 네트웍에 접근하는 접속장치의 설계 및 구현을 기술한다.

1. 서론

컴퓨터 제조 기술이 발달하면서 컴퓨터의 성능 면에서 비약적인 발전을 하였다. 이와 더불어 좀 더 작고 휴대하기 편한 컴퓨터의 요구가 증가하고 있다. 또한 네트워크의 확산으로 전 세계 어디에서나 쉽게 인터넷에 연결하여 다른 컴퓨터와 자료를 주고받을 수 있게 되었다. 그러나 네트워크에 연결된 컴퓨터는 다른 컴퓨터로부터 구별시킬 수 있도록 고유의 식별자를 가지도록 되어 있으며, 이 식별자는 물리적인 이더넷 주소 (MAC; Media Access Control address)와 논리적인 IP 주소로 구성되어 있다. 물리적인 이더넷 주소는 컴퓨터 또는 이더넷 장치의 제조 당시 결정되는 것으로써 일반 사용자는 고려하지 않아도 된다. 그러나 IP 주소는 국제 네트워크 정보 센터 (NIC; Network Information Center)에서 관리하여 전 세계적으로 유일하게 유지되고 있다. 따라서 국제회의에 참석하거나 업무상 출장 가는 회사원과 같이 이동형 컴퓨터를 이용하여 접속하는 환경이 자주 변하는 경우, 그 때마다 컴퓨터의 IP 설정을 변경해주는 번거로움이 생긴다. 이러한 단점을 해소하기 위하여 DHCP (Dynamic Host Configuration Protocol)나 NAT (Network Address Translator) 등의 개념이 제안되었다.

DHCP는 IP 주소를 비롯한 각종 TCP/IP 프로토콜 기본 설정을 개별 클라이언트들에 자동적으로 할당하는 방식의 프로토콜이다. 따라서 컴퓨터를 이용하고자 하는 네트워크 환경에서 DHCP를 제공한다면 이동형 컴퓨터에서는 DHCP 클라이언트로 설정을 하면 IP 주소는 자동으로 할당받게 된다. 이와 같이 자동으로 IP 주소를 할당받게 되어 있는 경우에도 IP 주소는 공식적으로 네트워크 IP 주소를 NIC로부터 할당받으며 자동적으로 IP 주소를 설정할 수 있는 범위를 제한하여야 한다. 따라서 공식적인 IP 주소가 부족한 경우 인터넷 환경에 접속할 수 있는 컴퓨터의 수가 제약을 받게 된다. 이러한 문제점을 극복하기 위하여 NAT의 개념이 도입되었다. NAT라는 것은 전송

되는 패킷의 시작 IP 주소나 목적 IP 주소를 변경하여 전송하고 수신함으로써 부족한 IP 주소 문제나, 방화벽(firewall), proxy 등에 사용하는 방법이다. 이 경우에도 일반적으로 내부 네트워크의 IP 주소는 라우터에서 전달되지 않는 사설 IP 주소 집단으로 설정하여야 하기 때문에 컴퓨터의 설정을 변경하여야 한다.

본 연구에서는 이러한 문제점들을 극복하고 사용자에게 편의성을 높이기 위하여 기존의 네트워크 환경을 그대로 유지하면서 인터넷 환경에 접속할 수 있는 방법을 제안한다. 제안된 접속장치를 PC게이트라고 부르며 NAT 개념의 일종인 IP 마스커레이딩 (IP Masquerading)을 통하여 사용자가 다른 환경에서 사용하던 컴퓨터를 기존 설정의 변경 없이 네트워크 환경에 접속할 수 있도록 Plug & Play 방식으로 구현되었다. 이 방식은 네트워크 접속을 허용하는 Linux 서버가 접속된 컴퓨터의 IP 주소를 판단하여 그에 대응되는 게이트웨이(gateway) 환경을 자동으로 설정하도록 한다. 이 방법을 통하여 사용자의 컴퓨터가 고정 IP 주소 (static IP address)를 사용하는지 동적 IP 주소(dynamic IP address)를 사용하는지에 상관없이 대상 컴퓨터의 설정을 변경하지 않고 인터넷에 접속할 수 있게 된다. 프로토타입 시스템의 구현을 통하여 정상적으로 동작함을 확인하였고 성능을 평가하였다.

2. 관련 연구

2.1. DHCP

DHCP는 IP 주소 뿐만 아니라 디폴트 게이트웨이 주소, DNS 서버 주소, 도메인 이름 등 각종 TCP/IP 프로토콜의 기본 설정을 개별 클라이언트들에 자동적으로 할당하는 방식의 프로토콜이다. 이외에도 DHCP 설정에는 많은 옵션들이 포함되어 있으나, 일반적으로 DHCP를 사용하는 윈도우 클라이언트들은 IP 주소의 수동 할당만 선택할 수 있다. 따라서 DHCP는 네트워크를 운용하는 데 필요한 TCP/IP 설정을 자동 관리하며, 개별 시스템에 IP 주소와 관련된 설정 정보를 부여한다고 할 수 있으며, 구성은 DHCP 클라이언트와 서버로 이루어진다.

DHCP 클라이언트는 시스템이 시작하면 DHCP 서버에 자신의 시스템을 위한 IP 주소를 요청한다. DHCP 서버로부터 IP 주소를 대여 받게 되면 TCP/IP 설정은 초기화되고 다른 호스트와 TCP/IP 프로토콜을 사용해서 통신할 수 있게 된다. 반면 DHCP 서버는 DHCP 클라이언트로부터 IP 주소 대여 요청에 응답하여 할당 가능한 IP 주소를 클라이언트에게 지정한다. 그러기 위해서는 DHCP는 미리 공인된 IP 주소 할당 기관으로부터 할당 가능한 IP 주소들의 영역 (scope) 만큼의 IP 주소를 미리 할당받아야 한다. 따라서 DHCP 단독으로는 IP 부족과 문제점들을 해결할 수 없어 NAT가 제안되었다.

2.2. NAT

일반적으로 어떤 호스트에서 다른 호스트로 통신을 하고자 할 때 전달되는 패킷에는 시작 IP의 주소와 목적 IP 주소가 기입되며, 데이터가 포함된다. 따라서 공인된 IP 주소의 부족 현상이 발생할 때, 이들 시작 IP 주소 또는 목적 IP 주소를 변경하여 한 컴퓨터에서 패킷이 전송되거나 또는 수신되는 것처럼 할 수 있다. 바로 이와 같이 시작 또는 목적 IP 주소를 변경하는 장치를 NAT라 한다. NAT는 OSI 모델의 3계층인 네트워크 계층에서 라우터에서 전달되지 않는 사설 IP 주소를 공인 IP 주소로 변환하는데 사용하는 통신망의 주소 변환기이다.

NAT를 사용하는 목적에는 2가지가 있는데, 첫째는 등록된 IP 주소를 절약할 수 있다는 점이고 둘째는 인터넷이란 외부 네트워크와 연결되는 사용자들의 고유한 내부 네트워크를 침입자들로부터 보호할 수 있다는 점이다. 등록된 IP 주소는 한정되어 있기 때문에 가급적 이를 공유할 수 있도록 하는 것이 필요한데 NAT를 이용하면 사설 IP 주소를 사용하면서 이를 공인 IP 주소와 상호 변환할 수 있도록 하여 공인 IP 주소를 다수가 함께 사용할 수 있도록 함으로써 이를 절약할 수 있는 것이다. 또는 인터넷과 내부 네트워크 사이에 방화벽 을 설치하여 외부 공격으로부터 사용자의 통신망을 보호하는 기본적인 수단으로 활용할 수 있다. 이 때 외부 통신망 즉 인터넷과 연결하는 장비인 라우터에 NAT를 설정할 경우 라우터는 자신에게 할당된 공인 IP 주소만 외부로 알려지게 하고, 내부에서는 사설 IP 주소만 사용하도록 하여 필요시에 이를 서로 변환시켜 준다. 따라서 외부 침입자가 공격하기 위해서는 내부 네트워크의 사설 IP 주소를 알아야 하기 때문

에 공격이 불가능해져 내부 네트워크를 보호할 수 있다.

일반적으로 NAT는 두 형태로 구분될 수 있는데, 시작점 NAT(SNAT; Source NAT)와 목적지 NAT(DNAT; Destination NAT)이다. SNAT는 첫 패킷의 시작 IP 주소를 변경하는 것을 말하는 데, 내부 네트워크에서 게이트웨이로의 라우팅이 발생한 후에 이루어지며 패킷이 바깥으로 나가기 직전에 행해진다. 일반적으로 알려진 마스커레이딩은 SNAT의 특별한 형태이다. 반면 DNAT는 첫 패킷의 목적 IP 주소를 변경하는 것을 말한다. 즉, 접속되는 패킷의 목적지를 변경하는 것이다. 따라서 DNAT는 외부 네트워크로부터 패킷이 전달되면 패킷의 목적 IP 주소를 바꾼 후, 라우팅 작업을 진행한다. 따라서 SNAT는 패킷의 시작 주소를 감추는 것이고, DNAT는 패킷의 목적지를 변경하여 내부 컴퓨터의 부하를 분산하거나 외부로 공개된 포트에 전송되는 데이터를 비공개 포트로 전달, 또는 투명한 프록시를 구성할 때 사용되는 방식이다.

그러나 NAT의 구현 시 내부 네트워크의 IP 주소는 라우팅에 포함되지 않는 사설 IP 주소를 위주로 설계되었기 때문에, 외부 네트워크 환경에서 사용하던 컴퓨터를 내부 네트워크에 접속하려고 할 때 마찬가지로 컴퓨터의 IP 설정을 변경하여야 한다. 따라서 본 연구에서는 외부 네트워크에서 사용하는 방식에 상관없이, 즉, DHCP를 이용하여 IP 주소를 자동으로 할당받아서 사용하던 환경이나 고정 IP 주소를 설정하여 사용하던 환경에 상관없이 접속되는 게이트웨이의 환경 정보를 자동적으로 변경하여 사용자가 IP 설정의 복잡함을 느끼지 않도록 SNAT와 DNAT를 이용하여 서버를 구축하였다.

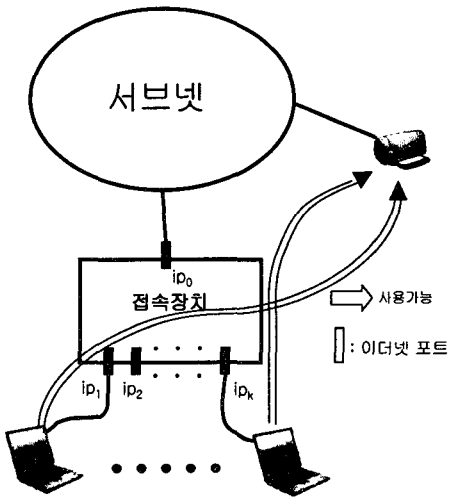
3. 설계 및 구현

본 절에서는 PC게이트의 설계 및 구현에 대하여 기술한다. PC게이트는 호텔이나 학회발표장 등에서 사용되는 것을 가정하고 있다. 먼저, PC게이트의 설계 시 고려사항을 분석하며 시스템 구성을 설명한다. 그리고 시스템의 구현 시에 문제점들에 대하여 설명한다.

3.1. 요구 분석

PC게이트는 여행자가 자신의 노트북으로 인터넷에 접속할 때 접속장치에 연결만 하면 여타의 설정없이 바로 인터넷에 접속할 수 있는 Plug&Play 기능을 지원한다. 설계 시 고려사항은 다음과 같다.

그림 1 이더넷 접속장치 개념도



1) Plug&Play 방식의 접속을 지원한다.

노트북이 인터넷에 접속할 수 있는 상태에 있을 때 네트워 상태는 두 가지 중의 한가지 상태에 설정되어 있다고 할 수 있다. 첫째는 DHCP 프로토콜에 의하여 IP주소를 할당받는 것으로 설정돼 있는 것이고 다른 하나는 고정 IP주소를 갖는 경우이다. DHCP의 경우엔 서브넷 내의 DHCP 서버에 의하여 IP주소를 할당받을 수 있도록 하면 되나 고정 IP를 갖는 경우엔 노트북의 IP주소가 그림 1에서 볼 수 있는 것처럼 서브넷의 IP와 다르며 접속이 불가능하다. 본 연구의 목표인 PC게이트는 두 경우 모두 설정 변경 없이 접속하도록 처리하여야 한다.

2) 그림 1에서 볼 수 있는 것처럼 하나 이상의 노트북을 수용할 수 있도록 설계한다.

3) 그림에서 볼 수 있는 것처럼 노트북이 서브넷에 설치된 프린터를 찾아서 설치할 수 있도록 하여야 한다.

4) 소형, 저가격의 내장형 시스템으로 구현하여야 한다.

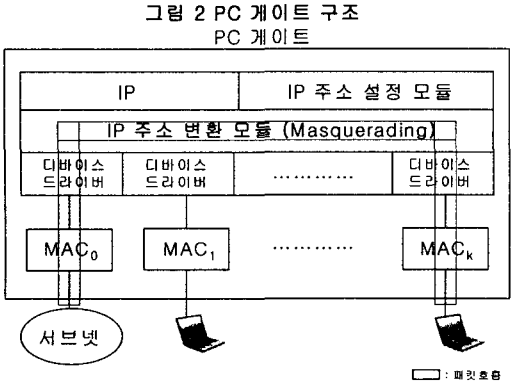
3.2. 설 계

DHCP의 경우 PC게이트가 DHCP 용 패킷을 여과없이 서브넷에 전달할 수 있으면 되므로 쉽게 문제를 해결할

수 있다. 문제가 되는 것은 사용자의 노트북이 고정 IP주소를 갖는 경우인데 이 경우 모든 패킷을 서브넷의 IP주소로 변환하여 서브넷으로 전송하고 서브넷으로부터 전달된 패킷도 해당 노트북의 IP로 변환해 주어야 한다.

이러한 기능을 수행하기 위하여 PC게이트는 그림 2와 같은 구조를 갖는다. 사용자의 노트북은 이더넷 MAC_{1-k}(Multiple Access Control) 칩에 연결되며 MAC_0 칩은 서브넷에 연결된다. 노트북의 패킷은 처음 접속했을 때 IP주소 설정 모듈의 도움을 받아서 IP 주소가 생성되며 이후엔 PC게이트의 IP주소변환모듈의 처리를 받아서 서브넷으로 전송된다.

그림 2 PC 게이트 구조



예를 들어 IP주소가 203.247.38.35으로 고정돼 있는 어떤 노트북이 MAC_i 칩에 접속되었다고 가정하자. MAC_i에 설정된 IP주소가 그 노트북의 주소와 같지 않으므로 노트북의 패킷은 PC게이트의 IP레벨까지 전달되지 못한다. PC게이트의 IP주소 설정 모듈은 노트북이 처음 접속되었을 때 해당 칩에 203.247.38.1 인 주소를 설정하여 이 문제를 해결한다.

3.3. 구 현

PC게이트는 내장형 시스템으로 설계되었고 저가격의 소형 시스템으로 구현해야 한다는 요구사항을 갖는다. 이를 위하여 CPU로서 MPC860을 선택하였다. MPC860은 모토롤라가 개발한 RISC 기반의 CPU로서 저가격이며 이더넷 콘트롤러를 2개 내장하고 있다. 일차적으로 노트북을 한 개만 접속하기로 한다면 매우 적절한 선택이라고 할 수 있다. 운영체제는 Embedded Linux를 사용한다. Embedded Linux는 TCP/IP프로토콜을 지원하고 개발환경도 좋기 때문에 PC게이트 구현에 적당하다.

구현은 Embedded Linux의 이더넷 디바이스 드라이버 부분과 IP부분을 수정하였다. 이더넷 디바이스 드라이버 부분에서는 초창기에 사용자의 패킷의 IP주소가 일치하지 않더라도 IP단계까지 패킷이 전달되도록 수정하는 것인데 모든 패킷을 받아들이도록 수정하였다. IP부분에는 IP 주소 설정 모듈을 추가하는 방식으로 수정하였다.

현재, PC 상에서 프로토타입 시스템이 구현되어 동작중에 있다. 서브넷에 존재하는 프린터는 PC의 컴퓨터 찾기 기능으로 찾아서 프린터 설치를 할 수 있으며 마스커레이딩에 의한 부담도 매우 작은 것으로 판단된다.

4. 결론 및 향후 연구 방향

본 연구에서는 사용자의 컴퓨터가 고정 IP 주소 (static IP address)를 사용하는지 동적 IP 주소(dynamic IP address)를 사용하는지에 상관없이 대상 컴퓨터의 설정을 변경하지 않고 인터넷에 접속하도록 허용하는 접속장치를 설계하고 구현하였다. 제안된 접속장치를 PC게이트라고 부르며 접속된 컴퓨터의 IP주소를 자동으로 판단하여 설정하고 NAT 개념의 일종인 IP 마스커레이딩 (IP Masquerading)을 통하여 패킷의 IP주소를 변환하도록 하였다. 현재 PC 기반의 프로토타입 시스템의 구현을 통하여 정상적으로 동작함을 확인하였고 마스커레이딩의 부담이 매우 적다는 것을 확인하였다. 향후에 이를 MPC860기반의 내장 시스템으로 이식할 예정이다.

참고 문헌

[1] "DHCP Options and BOOTP Vendor Extensions", RFC1533, www.ietf.org, W.Wimer. October 1993.

[2] "DHCP Options and BOOTP Vendor Extensions", RFC2132, www.ietf.org, S.Alexander.. March 1997.

[3] "The IP Network Address Translator (NAT)", RFC1631, www.ietf.org P.Prancis. May 1994.

[4] "MPC 860 Manual", www.motorola.com.