

리눅스 기반의 인터넷 공유기 개발

장성균⁰ 고정국
동명정보대학교 컴퓨터공학과
mrjang26@hanmail.net⁰, jgkoh@tit.ac.kr

Development of Linux-Based Internet Sharer

Sung-Gyun Jang⁰ Jeong-Gook Koh
Dept. of Computer Engineering, Tongmyong University of Information Technology

요 약

인터넷의 급속한 확산에 따라 각종 전자제품과 통신 장비의 보급이 가속화되면서 현재의 인터넷 주소체계로는 적절한 대응이 어려워졌고, 이러한 상황에서 IETF 가 인터넷 공유 기술을 공인하였다. 또한, 개인용 컴퓨터의 교체 주기도 점점 짧아지고 있다. 본 논문에서는 하나의 공인 IP 주소를 이용하여 다수의 단말 사용자들이 인터넷 서비스를 이용할 수 있도록 하는 인터넷 공유기를 개발하였다. 자원의 재활용을 위해 교체 후 방치되는 구형 PC 의 보드를 이용하여 개발된 인터넷 공유기는 개인이나 소규모 사무실에서 활용가치가 있을 것이다. 또한, 개발된 인터넷 공유기와 함께 사용자들이 손쉽게 인터넷 공유기를 제작할 수 있도록 하는 인터넷 공유기 유틸리티와 인터넷 공유기 소프트웨어도 함께 구현하였다.

1. 서 론

최근 인터넷의 급속한 확산과 통신 기술의 발달은 IT 산업의 급속한 성장을 촉진하고 있으며 이에 따라 각종 가전제품과 통신 장비의 개발 및 보급이 가속화되고 있다. 그러나, 현재의 인터넷 주소체계인 IPv4 로는 현재와 같은 인터넷 활용 범위의 급속한 증가 추세에 적절히 대응하기가 어려워 인터넷 통신규약 표준기관인 IETF 에서는 사용자들이 "가상의 사설 IP 주소 영역" 을 지정하여 사용할 수 있는 인터넷 공유 기술을 공인하고 있다.

한편, 90 년대 이후 컴퓨터 산업이 비약적으로 발전함에 따라 최신형 컴퓨터가 단기간에 구형 컴퓨터로 전락하는 등 PC 의 수명이 급격히 짧아지는 추세에 있다. 그러나 교체된 PC 는 대부분 버려지거나 방치되는 등 제대로 활용되지 못하는 상황이다.

본 논문에서는 하나의 공인 IP 주소를 이용하여 컴퓨터, IP 폰, 셋톱박스 등과 같은 다수의 단말 사용자가 동시에 인터넷 서비스를 이용할 수 있도록 하는 인터넷 공유기를 리눅스 기반으로 개발하였다. 한편, 가정이나 학교에서 최신형으로 교체한 후 방치되는 구형 PC 의 보드를 리눅스 기반의 인터넷 공유기 개발에 사용함으로써 버려지는 자원의 재활용이 가능하도록 하였다. 또한, 인터넷 공유기 유틸리티인 Creator 를 구현하여 사용자들이 손쉽게 인터넷 공유기 소프트웨어를 작성할 수 있도록 하였다.

본 논문의 구성은 다음과 같다. 2 장에서는 리눅스 기반의 인터넷 공유기가 제공할 기능들에 대해 기술한다. 3 장에서는 인터넷 공유기 구현 내역에

대해 기술하며, 4 장에서는 결론 및 향후 연구 방향을 서술한다.

2. 리눅스 기반의 인터넷 공유기 설계

본 논문에서는 리눅스 기반의 인터넷 공유기가 다음과 같은 기능을 제공하도록 설계하였다.

2.1 인터넷 공유 기능

Iptables 의 NAT(Network Address Translation) 테이블을 이용하여 패킷의 출발지 주소를 변경시키는 SNAT(Source NAT) 규칙을 적용함으로써 인터넷 공유(Masquerade) 기능을 제공한다. 한편, SNAT 는 패킷의 라우팅 경로를 결정한 후에 적용되는 Post-routing 기법이다. 즉, 패킷의 목적지 주소(www.gnu.org)에 근거하여 라우팅 경로가 결정된 상태에서 패킷이 호스트를 떠나기 전에 출발지 주소가 변경된다. 예를 들어, 내부 IP 주소가 192.168.0.2 인 호스트에서 www.gnu.org 의 서버에 연결을 시도하면 서버에 도달하는 패킷의 출발지 주소는 인터넷 공유기의 공인 IP 주소인 210.110.xxx.xxx 로 변경된다. 공인 IP 주소를 갖는 인터넷 공유기는 IP 마스크레이딩 기능을 이용하여 비공인 사설 IP 주소를 갖는 내부 네트워크의 다수 컴퓨터들이 동시에 인터넷을 이용할 수 있도록 한다[3].

2.2 포트 포워딩 기능

Iptables 의 NAT 테이블을 이용하여 DNAT(Destination NAT) 규칙을 적용함으로써 패킷의 목적지 주소를 변경시키는 포트 포워딩(Port Forwarding) 기

능을 제공한다. 예를 들어, jang@tit.ac.kr 에게 메일을 전송할 때 공유기에 도착한 패킷은 목적지 주소가 변경된 후 변경된 주소에 근거하여 새로운 라우팅 경로를 설정한다. 따라서, DNAT 는 Pre-Routing 기법이다[3].

2.3 방화벽 기능

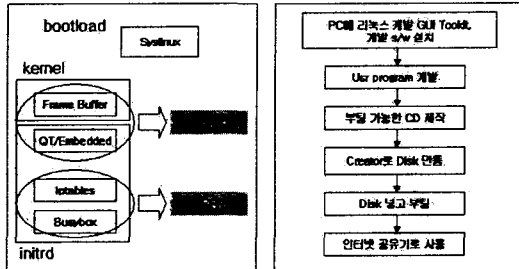
Iptables 의 NAT 테이블을 이용하여 DNAT 규칙을 적용함으로써 방화벽 기능을 제공한다. 즉, 내부 네트워크에서 외부 네트워크로 접속을 시도할 때 어떤 유형의 전송은 가능하게 하고 다른 유형의 전송은 불가능하게 한다.

3. 리눅스 기반의 인터넷 공유기 구현

3.1 구현 환경

인터넷 공유기를 구현하기 위해 호스트 컴퓨터의 운영체제로 레드햇 7.3 을 사용하였으며, 타겟 시스템은 구형 PC 를 사용하였다. 호스트 컴퓨터는 펜티엄-3 933MHz CPU, 256MB 메모리, 20GB 하드디스크, CD-Writer 이 장착되어 있다. AMD Pro-200MHz CPU, 32MB 메모리를 갖춘 타겟 시스템은 플로피 디스크 드라이브와 2 장의 네트워크 카드만 장착하고 있다.

리눅스 기반의 인터넷 공유기 유틸리티(Creator) 와 인터넷 공유기 소프트웨어(ISS : Internet Sharer Software)의 개발 과정은 [그림 1]과 같다.

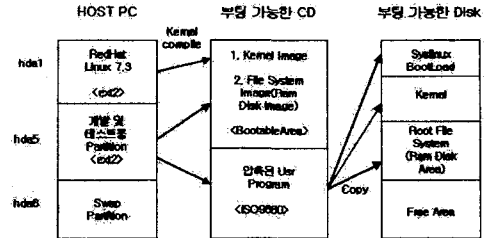


[그림 1] 인터넷 공유기 소프트웨어 개발 과정

호스트 컴퓨터의 하드 디스크는 [그림 2]와 같이 3 개의 파티션으로 구성되어 있다. Hda1 파티션에는 인터넷 공유기 개발 환경을 구축하기 위해 레드햇 7.3(전체 설치)과 인터넷 공유기 유틸리티 개발용으로 Qt/Embedded 3.0.5 버전을 설치하였다. 또한, Qt Designer 를 활용하기 위해 Qt/X11 3.0.5 버전도 설치하였으며, Multi-Call Binary 파일인 Busybox 와 부트 로더를 위한 SYSLINUX 도 함께 설치하였다. Hda5 파티션은 테스트용으로 CD 에 수록될 파일들을 구성하여 테스트함으로써 개발 기간을 단축할 수 있었다. Hda6 파티션은 스왑 파티션이다.

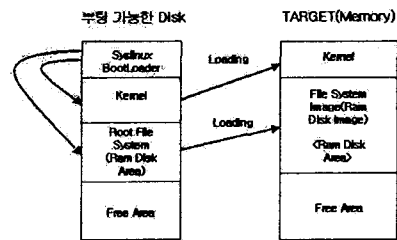
우선, CD-ROM 부팅이 가능한 컴퓨터에서 인터넷 공유기 유틸리티가 자동적으로 실행될 수 있도록 부팅용 CD 를 작성하며, 커널에서 Frame Buffer 를 지원하도록 설정하였다. 압축된 사용자 프로그램으

로 CREATOR 와 ISS 가 담겨진다.



[그림 2] 인터넷 공유기 개발 과정

다음으로, CD-ROM 부팅이 가능한 컴퓨터에서 부팅 후 자동으로 Creator 가 실행되면서 네트워크 환경 정보를 설정하면 ISS 가 플로피 디스크에 생성된다. 부팅용 플로피 디스크를 생성한 후 인터넷 공유기로 사용될 타겟 시스템에서 플로피 디스크로 부팅을 하면 [그림 2]와 같이 SYSLINUX 부트 로더가 커널과 루트 파일 시스템을 메모리에 적재하며, Iptables 를 실행하여 패킷 필터링 기능을 설정한다. 인터넷 공유기의 메모리 구성은 [그림 3]과 같다.



[그림 3] 인터넷 공유기의 메모리 구성

3.2 인터넷 공유기 소프트웨어

인터넷 공유기 소프트웨어에서 라우팅 정보와 게이트웨이 정보는 CREATOR 에서 설정한 내용이 수록된다.

넷필터는 패킷 필터링 기능을 구현하는 두 부분으로 구성된다. 첫번째 부분은 커널 영역의 필터링 기능 설정이다. 리눅스 커널 구성시에 필터링 기능을 포함하도록 설정한 후 커널을 재컴파일하여 커널 이미지를 생성한다. 두번째 부분은 필터링 규칙 설정이다. 필터링 규칙은 내부 네트워크에서 시스템 내외부로 새로운 연결을 설정할 수 있게 하고, 내부로 새로운 연결을 설정하거나 유효하지 않은 패킷은 허용하지 않도록 설정한다[2].

```
iptables -A tcprules -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A tcprules -i ! eth0 -m state --state NEW -j ACCEPT
iptables -A tcprules -i eth0 -m state --state NEW,INVALID -j LOG --log-prefix "IPTABLES DROP"
iptables -A tcprules -i eth0 -m state --state NEW,INVALID -j DOOP
```

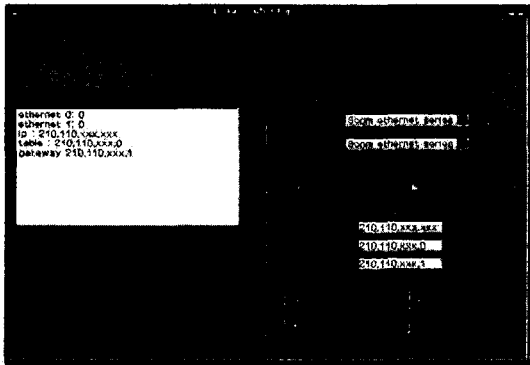
마스커레이딩 규칙은 다음과 같이 설정한다. SNAT는 Post-routing 방식이므로 패킷이 리눅스 박스를 떠나기 전에 출발지 주소가 변경된다.

```
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.0.0/24 -j SNAT --to-source 210.110.xxx.xxx
```

DNAT 를 이용한 포트 포워딩이 가능하도록 다음 규칙을 적용한다. 내부 IP 주소 192.168.0.2~192.168.0.6 은 웹 서버에게, 192.168.0.8~192.168.0.9 는 DNS 서버에게 부여하였다. 목적지 주소의 포트 번호 53 번과 80 번은 라우팅 이전 단계에서 변경하여 포트 포워딩이 되도록 하였다.

```
iptables -t nat -A PREROUTING -d 210.110.xxx.xxx -p tcp -dport 80 -j DNAT --to-destination 192.168.0.2-192.168.0.6:80
iptables -t nat -A PREROUTING -d 210.110.xxx.xxx -p tcp -dport 53 -j DNAT --to-destination 192.168.0.8-192.168.0.9
```

본 논문에서는 이러한 설정을 자동적으로 생성시켜 주는 인터넷 공유기 유틸리티인 CREATOR 를 [그림 4]와 같이 구현하였다. 사용자들은 이를 이용하여 네트워크 정보를 설정하면 설정 내역이 플로피 디스크에 담겨진다.



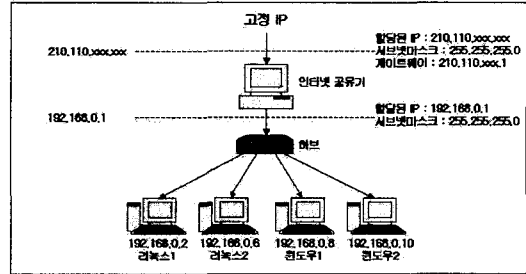
[그림 4] 인터넷 공유기 유틸리티의 화면 구성

네트워크 정보 설정 과정은 4 단계로 진행된다. 1 단계에서는 인터넷 공유기에 장착된 네트워크 카드의 종류를 선택한다. 현재 3Com, 인텔, 리얼텍 등의 6 가지 네트워크 카드를 선택할 수 있다. 2 단계에서는 IP 주소를 설정한다. 3 단계에서는 고정 IP 주소, 라우팅 및 게이트웨이 정보를 설정한다. 4 단계에서는 부팅 디스크 생성 작업을 수행하는 스크립트가 실행되는데, initrd 이미지를 생성하고 커널을 디스크에 복사한다.

3.3 인터넷 공유기의 기능 시험

CREATOR 를 이용하여 인터넷 공유기 소프트웨어를 작성할 경우 일반 사용자라도 인터넷 공유기를 쉽

게 구성할 수 있다. 개발된 인터넷 공유기의 기능을 시험하기 위한 시스템 구성은 [그림 5]와 같다.



[그림 5] 인터넷 공유기 기능 시험용 시스템 구성

인터넷 공유기의 기능 시험을 위해 내부 네트워크의 각 클라이언트에서 외부 네트워크에 대해 웹 서핑과 FTP 파일 송수신을 수행하였으며, 설계된 기능의 동작을 확인할 수 있었다.

방화벽 기능 시험시 외부에서 인터넷 공유기의 IP 주소로 ping 테스트 결과 응답이 없음을 확인하였다. 또한, 각 클라이언트에서 외부 IP 로 ping 테스트시 응답이 있었음을 확인할 수 있었다.

한편, 포트 포워딩 기능을 시험하기 위해 리눅스 1 과 2 에 웹 서버를 구축하고 홈 페이지 내용은 다르게 하였다. 외부에서 인터넷 공유기 주소로 접속을 시도하면 리눅스 1 과 2 의 홈 페이지가 번갈아가며 나오는 것을 확인하였다.

4. 결론 및 향후 연구 방향

본 논문에서는 개인 사용자나 소규모 사무실에 적합한 인터넷 공유기를 개발하고, 사용자들이 인터넷 공유기를 사용할 수 있도록 지원하는 유틸리티와 인터넷 공유기 소프트웨어를 구현하였다. 구형 PC 의 보드를 인터넷 공유기에 사용함으로써 버려지는 자원의 재활용이 가능하도록 하였다.

향후 연구 방향은 기존의 플로피 디스크 부팅 방식에서 플래쉬 메모리를 이용하는 임베디드 시스템이 되도록 변경하는 것이다.

참고문헌

- [1] Linux Kernel Compile Guide, http://kldp.org/KoreanDoc/2.4Kernel_compile-KLDP
- [2] RobBeck, " 넷필터로 구현하는 패킷 필터링 방화벽 수비", Linux@Work, 2001년 3월
- [3] 배철수, 커널 2.4 에서 NAT 구현, Linux@Work, 2001년 10월
- [4] Rusty Russell, 리눅스 패킷 필터링 하우투, 2000