MAC 주소를 이용한 IP 충돌 방지 기법의 설계 및 구현

김성걸, 임형석
전남대학교 정보통신협동과정
e-mail:sgkim@black.dongshinu.ac.kr
hslim@chonnam.chonnam.ac.kr

A Design and Implementation of IP Collision Preventive Method using MAC Address

Seong-Geol Kim, Hyeong-Seok Lim
Dept. of Interdisciplinary Program of Information and Telecommunication, Chonnam University

요 약

이 논문은 TCP/IP 기반의 근거리 네트워크에서 사용되는 개인용 컴퓨터의 MAC 주소을 이용하여 인터넷 프로토콜 주소 충돌을 해결하는 방법에 대하여 연구한다. 네트워크에 접속된 컴퓨터의 증가에 따른 IP 주소의 부족 현상과 고의 또는 실수로 권한을 받지 않은 사용자의 IP 주소의 사용에 의하여, 정당한 IP 주소 사용자가 네트워크를 사용할 수 없게 되는 경우가 있다. 본 논문은 근거리 네트워크에 접속되어 있는 컴퓨터의 MAC 주소와 IP 주소를 데이터베이스화 하여 IP 주소 충돌을 방지할 수 있는 시스템을 구축함으로써, 비정상적인 IP 사용자가 네트워크를 사용할 수 없도록 설계되어 있다.

1. 서론

본 논문은 근거리 네트워크 상에서 관리자에게 할당받지 않은 IP 주소를 사용자가 고의 또는 실수로 사용할 경우 사용 권한을 받은 사용자가 네트워크를 사용할 수 없게 되는 경우가 발생한다. 그 이유는 IP 주소는 고유성을 가지고 있기 때문에, 하나의 IP 주소를 여러 사용자가 사용하게 되면 먼저 IP 주소를 선점한 경우에는 사용할 수 있으나, 이후 동일한 IP 주소를 가지고 접속할 경우에는 IP 주소의 충돌로 인하여 네트워크의 접속이 차단되기 때문이다.

여러 사용자들의 MAC 주소와 IP 주소를 비교하여 IP 주소의 충돌을 해결한다는 것은 어렵다. 현재 시스템에 따라 NMS(Network Management System)에서 관리자에게 IP 주소의 충돌 메시지를 보여 주기는 하나, IP 주소를 할당받지 않은 비정상적인 사용자를 찾아서 해결한다는 것은 어렵다

이와 같은 문제를 해결하기 위해서 본 논문에서는 네트워크를 사용하고자 하는 사용자가 IP 주소의 사용을 요청할 경우에 네트워크의 관리자는 IP 주소의 사용 권한을 부여하여 정상적인 사용자의 안전한 네트워크를 보장한다. 그러나 비정상적인 사용자의 IP 주소의 사용을 방지하기 위하여 모든 네트워크 사용자가 고유하게 가지고 있는 MAC 주소와 IP 주소를 추출하여 데이터베이스화 하고, MAC 주소와 IP 주소가 일치하지 않을 경우, 그에 상응하는 메시지를 보여주고 비정상적인 사용자의 TCP/IP Winsock 컨트롤을를 비활성화 함으로써 네트워크 접속을 차단한다.

본 논문의 구성은 2장에서 네트워크 관리 프로토콜 및 인터페이스에 대하여 기술하고, 3장에서는 실질적인 시스템의 설계 및 구현 그리고 시스템에 대한 기대효과로 구성되어 있다. 마지막으로 4장에서는 본 연구에 대한 결론과 향후 연구방향에 대해서 서술한다.

2. 네트워크 관리 프로토콜 및 인터페이스

이 장에서는 네트워크의 전반적인 운영을 관리, 감독하는 시스템인 NMS와 Windows 환경 아래의 TCP/IP 표준 네트워크 인터페이스인 Winsock API에 대하여 기술하고자 한다.

* 본 논문은 한국과학재단의 특정기초연구(98-0102-11-01-3) 연구비 지원에 의한 것임

2.1 NMS(Network Management System)

네트웍 관리 시스템(Network Management System)이란 네트워크가 장애 없이 제대로 작동하고 있는지, 만일 네트워크에 부하가 걸려 있다면 그 이유는 무엇인지, 대역폭(bandwidth)의 사용은 무리가 없는지 등 네트워크 운영 전반에 관한 내용을 감독 및 관리하는 시스템이다. 이더넷, 토큰링, 프레임 릴레이, ATM 등 네트워크에 사용되는 카드, 허브, 스위치, 라우터, 서버 등 장비의 이상유무를 확인하여 대처할 수 있도록 지원하는 것이 바로 NMS다.

현재 공식적인 관리프로토콜은 크게 SNMP(Simple Network Management Protocol)와 CMIS/CMIP(Common Management Information System/Protocol) 등 2가지와 트래픽을 관찰하기 위하여 이용되는 RMON(Remote Network Monitoring)이 있다.

2.1.1 SNMP(Simple Network Management Protocol)

네트워크를 관리하고 네트워크 장비 및 그 기능을 모니터링 하는 표준 프로토콜로서 세부 사항들은 IETF(Internet Engineering Task Force)의 RFC(Requests for Comments)에 기술되어 있다.

SNMP[1] 패킷은 모든 표준 IP 라우터를 이용해 경로배정이 가능하므로 브리지와 라우터로 연결된 네트워크와 같은 네트워킹 환경관리에 이상적이다. SNMP는 여러 업체의 장비로 구성된 네트워크 관리의 표준이 되었다. 자신들의 네트워크 장비에 SNMP 에이전트를 지원하는 제조업자가 많을 뿐만 아니라 윈도우나 유닉스 시스템용의 다양한 중앙관리 소프트웨어 패키지가 존재한다.

2.1.2 CMIS/CMIP(Common Management Information System/Protocol)

최근 TMN(Telecomunication Management Network)이라는 개념이 도입되면서 CMIP/CMIS가 주목을 받고 있다.

CMIS(Common Management Information Service)는 시스템간 연결 및 해제를 위한 서비스인 A-Associate, A-Reases, A-Abort가 있고, 대리인에서 관리자에게 관리 객체에 발생한 특정 상황을 통지하는 M 이벤트 리포트 서비스가 있다. M 이벤트 리포트는 SNMP의 트랩과 같은 기능을 수행하나 이 메시지를 받은 관리자가 받았다는 확인을 해주어야 한다는 차이가 있다.

CMIP[2]는 관리정보를 전송하는 절차 즉 CMISE 사이에 CMIS 서비스를 완성시키기 위해서 교환하는 CMIP PDU를 만들고 전송하는 것에 대해 정의해 놓은 것이다. 관리 서비스를 위해서 CMISE는 PDU를 교환하기 위해서 CMIP를 채용한다. 그리고 CMIP는 CMIP PDU 전송을 위해서 ROSE(Remote Operations Service Element)를 이용하고 있다.

2.1.3 RMON(Remote Network Monitoring)

네트웍의 효율적 이용을 위해서 현재의 네트웍 상태를 측정하고 과거의 기록을 토대로 향후 네트웍 문제를 사전에 예측, 유용하게 이용되는 것이 RMON(Remote network MONitoring)[3]이다.

네트웍에서 발생한 트래픽 모두를 관찰하고자 나온 것이 네트웍 모니터링이다. 네트웍 데이터를 수집하는 대리인은 단독 장비 또는 웍스테이션 , PC, 허브, 스위치 등의 장비에 탑재하는 경우가 있다.

단독 장비는 모든 트래픽을 분석할 수 있으나, 별도로 구입함으로써 비용이 고가이고 기존장비에 탑재된 경우는 비용절감 효과는 있으나 장비 고유의 업무처리 때문에 트래픽을 정확하게 분석할 수 없다는 단점이 있다.

2.2 TCP/IP(Transmission Control Protocol/Internet Protocol)

TCP/IP[4]는 인터넷의 기본적인 통신 프로토콜로서, 인트라넷이나 엑스트라넷과 같은 통신 프로토콜로서 인트라넷이나 엑스트라넷과 같은 사설 망에서도 사용된다.

TCP/IP는 2개의 계층으로 이루어진 프로토콜이다. 상위계층인 TCP (Transmission Control Protocol)는 메시지나 파일들을 좀더 작은 패킷으로 나누어 인터넷을 통해 전송하는 일과, 수신된 패킷들을 원래의 메시지로 재조립하는 일을 담당한다. 하위계층, 즉 IP (Internet Protocol)는 각 패킷의 주소부분을 처리함으로써, 패킷들이 목적지에 정확하게 도달할 수 있게 한다. 네트워크상의 각 게이트웨이는 메시지를 어느 곳으로 전달해야 할 지를 알기 위해 메시지의 주소를 확인한다. 한 메시지가 여러 개의 패킷으로 나뉘어진 경우 각 패킷들은 서로 다른 경로를 통해 전달될 수 있으며, 그것들은 최종 목적지에서 재조립된다.

TCP/IP는 통신하는데 있어 클라이언트/서버 모델을 사용하는데, 컴퓨터 사용자(클라이언트)의 요구에 대응하여, 네트웍 상의 다른 컴퓨터(서버)가 웹 페이

지를 보내는 식의 서비스를 제공한다. TCP/IP는 본래 점대점(Point-to-Point) 통신을 하는데, 이는 각 통신이 네트웍 상의 한점(또는 호스트 컴퓨터)으로부터 시작되어, 다른 점 또는 호스트 컴퓨터로 전달된다는 것을 의미한다.

TCP/IP와 관련이 있는 프로토콜로 UDP (User Datagram Protocol)가 있는데, 이것은 특별한 목적을 위해 TCP 대신에 사용되는 것이다. 라우팅 정보를 교환하기 위해 네트웍 호스트 컴퓨터에 의해 사용되는 프로토콜에는 ICMP (Internet Control Message Protocol), IGP (Interior Gateway Protocol), EGP (Exterior Gateway Protocol), 그리고 BGP (Border Gateway Protocol) 등이 있다.

2.3 Winsock API

Windows Sockets Application Programming Interface(Winsock API)는 Berkeley Software Distribution of UNIX에 의해 대중화된 Sockets Interface를 수행하는 Function들의 Library이다. 개발 취지는 Windows 환경하에서 TCP/IP로의 표준화를 이끌어내기 위한 것이었다.

TCP/IP 기반의 통신 application을 위해 여러 가지의 programming interface가 개발되어 왔다. 그 중에 가장 널리 사용된 것은 Berkeley Sockets interface으로, Winsock은 Berkeley Sockets(BSD version 4.3)에 기초하고 있다.

WinSock은 Windows의 message-driven 속성을 지원하며 protocol에 독립적인 Berkeley socket의 수행을 지향한다.[4]

3. 시스템의 설계 및 구현

3.1. IP 충돌 방지를 위한 시스템의 설계

개인용 컴퓨터는 사용자가 고의 또는 실수로 자신의 IP 주소를 바꾸는 것에 아무런 제약이 없다. 자신에게 할당된 IP 주소가 아닌 것을 사용하여도 통신이 가능하며, IP 주소의 소유에 대한 제약이 없어서, 정당하게 IP 주소의 사용 권한을 받은 사용자의 네트워크 사용을 보호할 수 없다는데에 착안하여 이 시스템을 설계하였다.

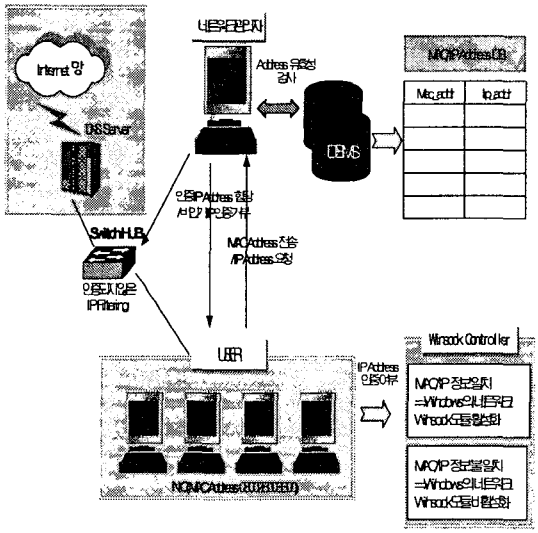
이 시스템의 설계의 전제 조건으로는 클라이언트 시스템의 MAC 주소와 IP 주소를 관리자가 서버의 데이터베이스로 관리하고 있어야 한다..

시스템의 설계는 3개의 범주로 구성되어 있다.

첫째로 클라이언트 시스템에서 MAC 주소와 IP 주소를 추출하는 부분이다.

둘째로 클라이언트에서 추출한 MAC 주소와 IP 주소가 서버의 데이터베이스에 저장하고 있는 MAC 주소와 IP 주소가 일치하는가 하는 유효성을 검사를 하는 단계이다.

셋째로 MAC 주소와 IP 주소가 불일치할 경우에는 사용자에게 메시지를 남기고 Winsock 컨트롤 모듈을 비활성화하여 네트워크의 사용을 차단하도록 설계 되어 있다.



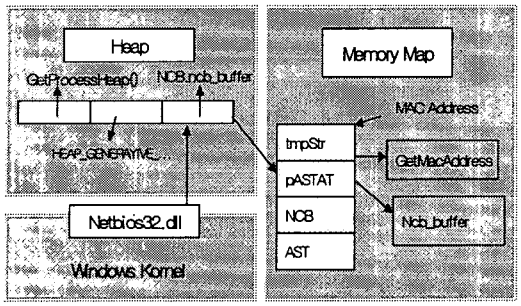
[그림 1] IP Address의 충돌방지를 위한 Server/Client 시스템의 구성도

3.2 구현

3.2.1 MAC 주소의 추출

MAC 주소는 OSI 7 Layer의 Data Link Layer에 속하는 NIC(Network Interface Card)에 할당된 유일한 주소로서 IEEE에 의해 제조업체에 할당되며 첫 번째 3바이트는 공통적으로 적용되고 나머지 3바이트는 제조업체에서 할당하는 총 6바이트로 구성되어 있다.

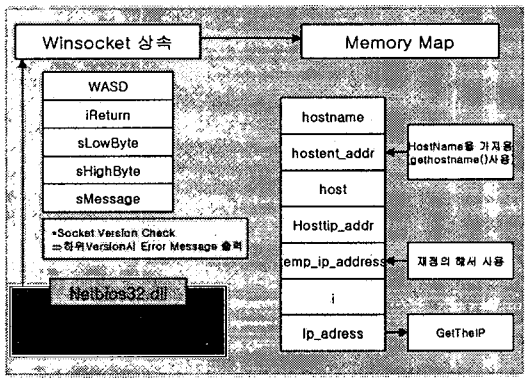
RARP(Reverse Address Resolution Protocol)[5]에 의해 Network 계층의 IP Address로 반환하기 위한 클라이언트의 MAC 주소를 추출하는 구성도는 다음과 같다.



[그림 2] MAC 주소 추출 구성도

3.2.2 IP 주소 추출

클라이언트에서 사용하고 있는 IP 주소를 추출하는 구성도는 다음과 같다.

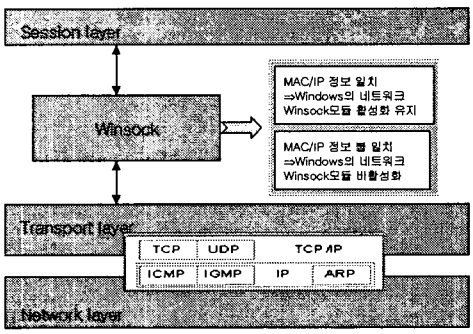


[그림 2] IP 주소 추출 구성도

여기에서 추출되는 IP 주소는 사용 권한 여부를 판단할 수 없으며, 단지 클라이언트에 설치된 상태를 파악할 수만 있다.

3.2.3 Winsock 활성화 구성도

Winsock은 OSI Transport layer와 Session layer 사이에 존재하면서 MAC Address와 IP Address 정보가 불일치할 경우에 Transport layer상에 존재하는 Winsock Controller를 종료한다.



[그림 2] Winsock Controller 구성도

3.3 시스템의 효과 및 한계

이 시스템은 근거리 네트워크 상에서 발생하는 IP 주소의 충돌을 방지할 수 있으나, 네트워크의 관리자는 IP 주소의 인증과 접속하는 사용자의 MAC 주소와 IP 주소를 관리하는 서버의 보안에도 효율적인 관리를 하여야 한다. 그리고 다른 IP 주소의 그룹에서 발생하는 문제에 대하여서는 관여할 수 없다는 한계성을 가지고 있다.

4. 결론 및 향후 연구 방향

본 연구에서는 네트워크에 접속하는 컴퓨터의 MAC 주소와 IP 주소를 데이터베이스화하여 고의 또는 불법으로 IP 주소를 사용하려는 사용자의 Winsock 콘트롤러를 강제로 종료함으로써 IP 주소의 충돌을 해결하였다. 그러나 동일한 IP 주소의 그룹에서만 IP 주소의 충돌을 방지할 수 있다는 한계성과 Winsock을 사용하지 않는 시스템에서는 적용되지 않는다는 한계성이 있으므로, Winsock을 사용하지 않는 시스템에서의 IP 주소의 충돌 문제와 여러 IP 주소의 그룹에서의 IP 주소의 충돌을 방지할 수 있는 계속적인 연구가 필요하다.

참고문헌

[1] J. Case, M. Fedor, M. Schoffstall, J. Davin"A Simple Network Management Protocol(SNMP)" RFC 1098, May 1990

[2] U. Warrier, L. LaBarre, L. Besaw, B. Handspicker, "The Common Management Information Services and Protocols for the Internet (CMOT and MIP)", RFC 1095,October 1990

[3] S. Waldbusser, "Remote Network Monitoring Management Information Base", RFC 1757, Carnegie Mellon University, February 1995

[4] McCoghrie, K., and M. Rose, "Mangement Information Base for Network Mangement of TCP/IP -based Internets", RFC 1066, TWG August 1988

[5] Finlayson, Mann, Mogul, Theimer, "A Reverse Address Resolution Protocol", RFC 903, Stanford University, June 1984