IP 주소 관리 시스템의 설계 및 구현

이희찬O, 이준형, 박진원, 김명균
울산대학교 컴퓨터정보통신공학부
{ dino3941O,comfuny }@cnlab.ulsan.ac.kr, zwsonic@shinbiro.com, mkkim@ulsan.ac.kr

Design and Implementation of IP address management system

HeeChan Lee O, JoonHyung Lee, Zinwon Park, MyungKyun Kim
Department of Computer Engineering and Information Technology, University of Ulsan

요 약

대규모의 네트워크를 사용하는 기업이나 학교, 기관에서는 IP주소의 효율적인 관리를 위해 여러 가지 노력을 하지만 사용자의 허가되지 않은 IP주소의 무단 사용에 대하여 대처할 방법이 마땅치 않다. 사용자 임의로 IP주소를 설정하여 사용하게 되면 이를 찾아내기가 매우 까다롭고, 만약 그 IP주소가 중요서버의 IP일 경우에는 IP주소의 중복사용으로 인한 서비스 장애가 발생할 수도 있다. 본 연구에서는 현재 네트워크 설정을 변경하지 않으면서 사용자의 특별한 개입 없이 IP주소를 관리 및 모니터링 하고 중요 서버의 IP사용을 보호할 수 있는 에이전트 기반의 시스템을 개발하고자 한다.

1. 서 론

Static IP를 사용하는 네트워크에서 IP주소의 중복사용으로 인한 문제는 흔히 발생하게 된다. 특히 중복 사용된 IP주소가 주요 서버이거나 라우터, 게이트웨이의 IP주소일 경우 서비스 장애가 발생하게 되는데 이를 대처할 방법이 마땅치 않다.

본 논문에서는 IP주소가 중복 사용되어서는 안될 주요 서버 및 라우터, 게이트웨이의 IP주소를 다른 호스트가 사용하지 못하도록 차단하는 IP 주소 관리 시스템을 설계하였다.

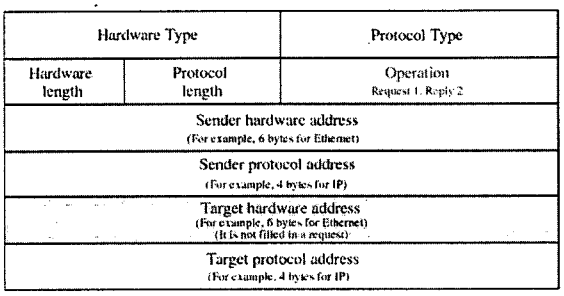
본 논문의 순서로는 2장에서 IP주소의 불법적인 사용을 차단하는 기법에 대하여 설명하고, 3장에서는 이를 기반으로 구현한 시스템의 구조를 설명하며, 4장에서는 시스템을 구현한 실험 결과를 보여주고, 마지막으로 5장에서는 결론을 제시한다.

2. 차단 기법

2.1. Gratuitous ARP 프로토콜

ARP[1]는 IP 주소체계를 기반으로 하는 네트워크 상에서 IP주소를 MAC주소에 대응시키기 위해 사용되는 프로토콜이다. 예를 들어 호스트 A가 호스트 B에게 IP 패킷을 전송하고자 할 때 같은 브로드캐스트 도메인에 있을 경우에는 호스트 B의 MAC주소를, 다른 브로드캐스트 도메인일 경우에는 그 네트워크의 라우터의 MAC주소를 알아야만 패킷을 전송 가능하다. 이 때 호스트 A는 호스트 B나 라우터의 MAC주소를 알기 위해 ARP 프로토콜을 사용하게 되는데 ARP의 Sender Hardware Address필드와 Sender Protocol Address필드에는 자신의 MAC주소와 IP주소를 넣고, Target Protocol Address에는 호스트 B나 라우터의 IP를 넣어서 ARP Request 패킷을 전송하여 호스트 B나 라우터의 하드웨어 주소(Target Hardware Address)를 얻을 수 있다. ARP Request를 받은 호스트는 ARP Reply를 전송하게 되고, 이 과정을 통해 호스트 A는 상대방의 MAC주소를 알아낸다. [그림1]은 ARP 패킷의 구조를 보여주고 있다.

Gratuitous ARP[2]는 컴퓨터가 온라인(부팅)상태가 될 때나 IP 소프트웨어가 초기화 될 때(IP 주소를 바꿨을 경우) 네트워크 상에 같은 IP 주소를 사용하는 호스트가 있는지 검사할 때 사용하는 방법이다. Gratuitous ARP는 Sender, Destination Protocol Address필드에 자기의 IP 주소를 똑같이 입력하고 Sender Hardware Address필드에는 자신의 MAC 주소, Destination Hardware Address 필드에는 00:00:00:00:00:00을 입력하여 네트워크 상에 ARP Request(Gratuitous ARP)전송



[그림1] ARP Protocol

을 하게 되고 이 패킷에 대한 ARP Reply가 오면 네트워크 상에 자신과 같은 IP 주소가 있다는 것을 인지하여

IP 주소 획득에 실패한다.

본 연구에서는 Gratuitous ARP를 사용하여 차단 하여야 할 IP의 Gratuitous ARP 패킷을 검출 하였을 경우 에이전트가 임의의 ARP Reply를 생성하여 전송함으로써 차단할 호스트의 네트워크 초기 설정을 막아 비인가된 IP 사용을 차단하는 기법을 사용하였다.

2.2. ARP Spoofing

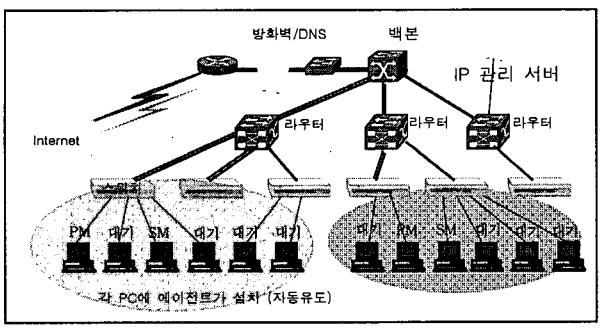
본 연구에서는 Gratuitous ARP로 차단에 실패하였을 경우(네트워크 설정 후 네트워크에 연결하는 경우) ARP Spoofing[3]을 사용하여 IP주소의 사용을 차단한다. ARP Spoofing 이란 어떤 사용자가 자신의 MAC주소를 다른 호스트의 MAC주소로 설정하여 ARP 패킷을 구성하여 네트워크에 주기적으로 전송함으로써 네트워크의 다른 호스트들에게 자신이 다른 호스트인 것처럼 위장하는 기법이다.

본 연구에서 에이전트는 차단하고자 하는 IP주소의 ARP Request 패킷을 검출하였을 경우 다른 호스트들의 ARP Cache Table을 변경하기 위하여 Spoofing된 ARP Reply를 네트워크에 전송하여 차단하고자 하는 호스트와 다른 호스트들과의 연결을 차단시킴으로써 네트워크의 연결을 막아 IP의 사용을 제한하는 기법을 사용하였다.

3. 시스템 설계

3.1. 시스템 구조

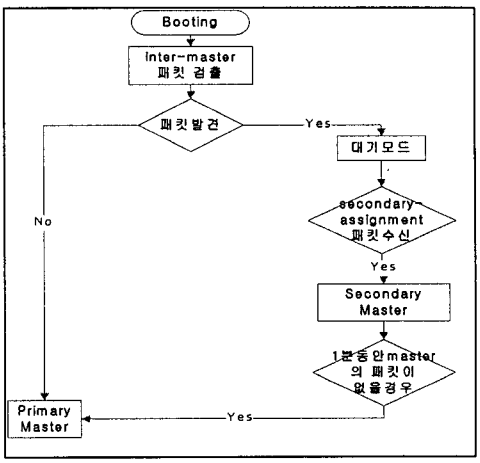
시스템은 네트워크 전체에 걸쳐 하나의 IP주소관리 서버가 존재하게 되고, 네트워크에 속하는 모든 호스트에는 에이전트가 설치된다. 각 브로드캐스트 도메인에는 하나의 PM(Primary Master)모드로 동작하는 에이전트와 하나의 SM(Secondary Master)모드로 동작하는 에이전트가 선정되고 나머지 에이전트들은 대기모드로 작동하게 된다. IP관리서버는 PM모드로 동작 중인 에이전트로부터 데이터를 수집하고, 관리자에 의해 수정된 관리정책을 PM에게 전송하는 역할을 한다. [그림2]는 전체 시스템에 대한 구상도이다.



[그림2] 전체 시스템 구상도

3.2. 에이전트

본 논문의 차단 기법은 브로드캐스트 되는ARP패킷을 기반으로 하고 있기 때문에 각 브로드캐스트 도메인을 단위로 하나의 에이전트 집단을 형성하게 된다. PM모드로 동작하는 에이전트는 시작 시 IP관리서버에 연결하여 차단 해야 할 IP주소-MAC주소 맵핑 테이블을 가져오게된다. PM모드로 동작하는 에이전트는 ARP패킷을 캡쳐하게되고, 차단 해야 할 IP주소의 ARP일 경우 MAC주소를 검사하여 등록된 MAC주소와 다를 경우 불법적인 IP사용으로 간주하여 그 호스트를 차단하게 된다. IP관리서버에 주기적으로 네트워크의 상태를 전송하게 된다.



[그림3] 에이전트의 처리 과정

또한, 시스템의 견고성을 높이기 위해 에이전트는 Primary-Secondary의 구조를 가지고 있다. 에이전트는 시작이 자신의 브로드캐스트 도메인에 PM모드로 동작중인 에이전트가 있는지 검사를 한다. PM모드로 동작중인 에이전트가 없을 경우에는 자신이 PM모드로 작동하게 되고, PM모드로 동작 중인 에이전트가 이미 존재한다면 자신은 대기모드로 작동하게 된다. PM모드로 작동하는 에이전트는 자신이 수집한 IP List중에서 랜덤하게 한 호스트를 설정하여 Secondary Master로 지정하고 그 호스트의 에이전트에게 Secondary Master로 동작하라는 메시지를 전달하게 된다. SM에이전트는 PM에이전트과 주기적인 통신을 통해 PM이 가지고 있는

Using IP List Reply

Type(0x01)	Length	IP_1	IP_2	IP_3

Using IP List Request

Type(0x02)

Secondary Master Mode지정

Type(0x03)

PM Find Request

Type(0x04)

PM Find Reply

Type(0x05)

[그림4] 에이전트간의 메시지 포멧

리스트를 저장하고, PM이 일정시간 동안 응답이 없을 경우 PM이 종료된 것으로 간주하고 자신이 PM으로 전환하게 된다. [그림3]는 에이전트의 처리 과정이다..

각 에이전트들은 PM로 동작하는 에이전트가 있는지에 대한 검사, PM가 대기모드인 에이전트에게 SM로 동작하도록 명령하는 명령, PM와 SA간의 데이터 송수신 등에 관련된 메시지를 주고 받고, PM로 동작 시 전체 네트워크를 관리하는 서버인 IP관리서버와의 통신을 통해서 필요한 데이터를 송수신 하기 위해 UDP/IP를 사용하고 [그림4]와 같은 메시지 포멧을 사용하였다.

3.3. IP관리서버

IP관리서버는 관리하는 네트워크에 단 한대만 존재하게 된다. IP관리서버는 PM에게 IP주소-MAC주소 맵핑 테이블을 전달하고, PM들로부터 현재 네트워크 상태를 전달받아 관리자에게 정보를 제공하는 기능을 하게 된다. 또한 관리자로부터 관리정책을 입력 받아 변경된 관리정책을 PM으로 전달하는 기능을 맡게 된다. [그림5]는 IP관리서버와 PM사이에서 사용하는 메시지 포멧이다.

Request Block List

Type(0x11)	PM IP

Reply Block List

Type(0x12)	Length	IP_1	MAC_1	IP_2	MAC_2

Request Using IP List

Type(0x13)	PM IP

Reply Using IP List

Type(0x14)	Length	IP_1	MAC_1	IP_2	MAC_2

[그림5] 에이전트-IP관리서버 간 메시지 포멧

4. 실험 결과

앞에서 설명한 IP 주소 관리 시스템을 구현하여 실제 네트워크에 적용하여 중요서버의 IP주소가 보호되는지 실험하였다. IP 관리 서버는 서버들의 IP주소를 가지고 있으며 PM에이전트는 해당 IP 주소를 사용하려 시도하는 호스트에 spoofing된 ARP를 전달하여 IP주소의 사용을 제한하는 것을 확인하였다. 아래의 [그림6]은 IP 관리 서버가 보유한 IP 주소 목록을 보여주고 있으며 [그림7]은 PM에 쌓인 로그파일의 일부분을 보여주고 있다.

```
Group_01
192.168.0.5
192.168.0.20
192.168.0.120
Group_02
192.168.1.8
192.168.1.34
192.168.1.65
```

[그림6] IP관리서버의 Using IP List

```
Detect 192.168.0.2 Gratuitous ARP
  → Send ARP Reply
Detect 192.168.0.134 RequestARP
  → Send ARP Reply
Detect 192.168.0.122 Gratuitous ARP
Detect 192.168.0.95 Gratuitous ARP
Detect 192.168.0.212 Gratuitous ARP
  → Send ARP Reply
```

[그림7] 에이전트의 로그파일

5. 결론

본 논문에서는 서버에서 사용되는 IP를 다른 호스트에서 임의로 사용하는 문제점을 해결하는데 초점을 두고 IP관리시스템을 개발하였다. 본 시스템에서는 IP관리서버와 에이전트를 기반으로 네트워크의 중요한 IP를 보호하게 되며, 에이전트가 일시적 장애를 일으키는 경우를 대비하여 Primary-Secondary의 구조를 가지게 설계하여 시스템의 견고성을 높였다.

향후 연구에서는 시스템에서 필요한 메시지의 종류를 좀 더 세분화 하고, PM으로부터 IP관리서버로 좀 더 세분화된 네트워크의 상태를 전달하고자 한다. 또한, 에이전트의 기능을 모듈화 하여 기존에 이미 사용하고 있는 시스템들에 추가하여 사용할수록 있도록 하여 시스템의 활용도를 높이고자 한다..

참고문헌

[1] D.C. Plummer, An Ethernet Address Resolution Protocol, RFC826, November, 1982

[2] T.-S. Jou, "Duplicate IP Address Detection Based on Gratuitous ARP", February, 1999

[3] Sean Whalen, An Introduction to Arp Spoofing, http://packetstormsecurity.nl/papers/protocols/intro_to_arp_spoofing.pdf, 2001