VLAN 환경에서 네트워크 주소 인증을 통한 정책 기반 실시간 시스템 제어 기술 연구

최원우* · 안성진** · 정진욱*

요 약

네트워크(IP/MAC) 주소를 관리함에 있어 네트워크의 임의의사용자가 사용자가 사용 중인 네트워크 장비 혹은 PC의 IP 주소나 네트워크 인터페이스 카드를 임의적으로 또는 악의적으로 변경하는 것을 차단할 필요성이 있다. 또한 새로운 네트워크 자원 장비의 도입 시 수많은 네트워크 자원을 임의적으로 할당하지 않고, 관리자가 관리하게 됨으로써 효율적인 자원관리 및 네트워크 문제 발생시 신속한 대처를 할 수 있어야 한다. 이것은 하위레벨에서의 네트워크 관리 및 보안을 유지할 수 있게 한다. 그러나 이러한 작업을 현재는 대부분 관리자에 의한 수작업으로 진행하고 있으며 이로 인한 관리 인력의 낭비와 업무능률의 저하는 관리효율 자체의 저하로 이어진다. 본 논문에서는 기업이나 관공서에서 사용되는 VLAN 환경에서 네트워크 주소 인증을 통해 보안성을 더욱 향상시키기 위한 방안을 제시하고자 한다.

A Study on the Network Access Control of a System in Real Time by Network Address Authentication Based on Policy in the VLAN Environments

Won Woo Choi* · Seong Jin Ahn** · Jin Wook Chung*

ABSTRACT

It is need to control network access that a user personally change own IP or network devices in managing network address. Also, When we use new network devices or assign network address, we do them by design, not arbitrarily. And then, we can immediately control network's problems. It could be used network management and security in low level. But most of managers do this works by hand not automatically. This paper propose the solutions that improve the security by network address authentication in VLAN environment, such as corporations and public offices.

Key words : VLAN, Network Address, Authentication

* 성균관대학교 컴퓨터공학과

** 성균관대학교 컴퓨터 교육학과

1. 서 론

대규모 분산 네트워크를 사용하는 기업, 연구소, 학교 등의 전산 관리자들은 수많은 IP 주소를 관리하기 위해서 엄청난 시간과 비용을 소모하고 있음에도 불구하고 효율적인 IP 주소 관리가 이루어지지 못하는 경우가 대부분이다. 이 결과로 몇몇 개인 사용자들은 자신의 임의대로 허가 받지 않은 IP 주소를 사용, 네트워크와 인터넷에 접속하여 내부 정책에 위반이 되는 행위를 하기도 하며 다른 IP와 충돌을 유발함으로써 네트워크에 치명적인 장애를 유발하기도 한다. 네트워크에 존재하는 모든 IP 주소와 MAC주소, 그리고 사용자 이름을 동시에 관리함으로써 네트워크 자원의 보안성, 효율성, 생산성을 높이는 노력이 필요하다.

IP/MAC 주소를 관리함으로써 네트워크의 임의의 사용자가 사용중인 네트워크 장비 혹은 PC의 IP 주소나 네트워크 인터페이스 카드를 임의적으로 또는 악의적으로 변경하는 것을 차단할 수 있다. 또한 새로운 네트워크 자원 장비의 도입 시 수많은 네트워크 자원을 임의적으로 할당하지 않고, 관리자가 관리하게 됨으로써 효율적인 자원관리 및 네트워크 문제 발생시 신속한 대처를 할 수 있다. 이것은 하위레벨에서의 네트워크 관리 및 보안을 유지할 수 있게 한다. 그러나 이러한 작업을 현재는 대부분 관리자에 의한 수작업으로 진행하고 있으며 이로 인한 관리 인력의 낭비와 업무능률의 저하는 관리효율 자체의 저하로 이어진다. 네트워크가 방대해 짐에 따라 이러한 문제는 더욱 치명적인 문제점으로 나타날 것이다. 그러므로 이러한 작업을 전산화하고 자동화하는 것은 관리자에게 보다 능률적으로 관리업무에 몰입할 수 있는 환경을 제공할 것이며 관리 인력의 낭비를 막을 수 있다. 또한 앞으로 직면하게 될 IP 주소 부족 현상에 보다 탄력적으로 대처할 수 있으며 IPv6 방대한 주소체계를 관리하는데 있어서는 반드시 구축되어야 할 시스템이다.

2. 네트워크 주소인증의 필요성

네트워크 프로토콜의 취약점을 이용한 네트워크와 네트워크 시스템에 대한 피해가 날로 심각해지고 있다. 비록 네트워크에 대한 접근이 모든 사용자에게 개방되어 있기 때문에 네트워크 관리나 보안적은 측면에서 단계별로 접근에 대한 제한을 둘 필요가 있다. 하지만 네트워크로의 접근 관점에서 볼 때 비인가된 사용자의 접근을 방지하기란 쉬운 일이 아니다.

IP/MAC주소를 매핑한 사용자를 네트워크 자원으로 규정할 때 기존의 네트워크 주소관리 운영의 문제점은 다음과 같다.

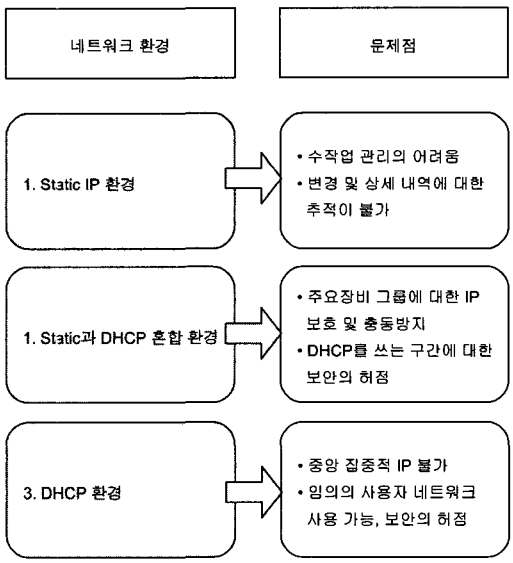
- 네트워크 자원의 수동관리로 인한 인적 자원 낭비 및 업무 능률 저하
- 인가된 IP 주소에 대한 사용/미사용 모니터링 수단 부재
- 비인가 IP 주소에 대한 사용 통제 수단 부재 내부 사용자의 IP도용에 따른 장애 및 내부 보안 문제 발생
- 네트워크 장애시 IP/MAC 주소에 대한 물리적 위치 매핑 수단 부재
- 실시간 IP 자원 파악 및 증설 결정시 근거 자료 부재
- 미 할당 IP에 대한 접근 통제 부재

2.1 네트워크 환경에 따른 주소 관리 문제점

네트워크 환경에 따른 주소 관리의 문제점은 다음과 같이 정리해 볼 수 있다.

날로 더해 가는 네트워크의 대규모화에 따라 그의 관리는 중요한 이슈가 되고 있다. 이러한

측면에서 현재 수많은 네트워크 관리 시스템들이 선보이고 있지만 대부분의 시스템은 네트워크의 자원인 IP/MAC 주소에 대한 관리는 소홀히 하고 있는 것이 사실이다. 이러한 현상은 네트워크 보안을 취약하게 만들고 있으며 IP 주소 충돌로 인한 장애에 대해서 마땅히 예방할 방법을 제공하고 있지 못하다. 이에 본 논문에서는 IP/MAC 주소의 통합 관리에 초점을 맞추어 네트워크의 보안성을 향상시키고 IP 주소의 임의적 변경 또는 악의적 사용에 의한 각종 장애에 대처할 수 있는 기능을 제공함으로써 IP 주소 충돌로 인한 네트워크 장해 요인을 제거하여 보다 효과적인 IP/MAC 주소 관리를 도울 수 있다. 네트워크 주소 사용에 대한 투명성 확보, IP 주소의 충돌로 인한 장애 발생 제거, 비인가 IP에 대한 사용을 사전에 차단할 수 있으며, 네트워크 관리 시스템(NMS : Network Management System)과의 연동으로 장애에 대한 보다 신속한 조치가 가능하며 대규모 관리의 효율성을 극대화 시킬 수 있다.



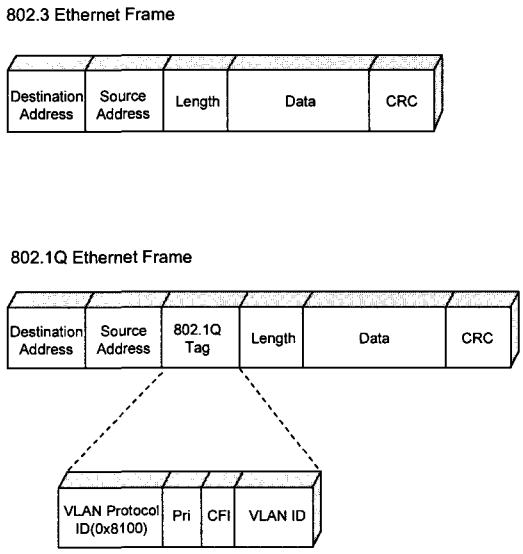
(그림 1) 네트워크 주소관리 보안상 문제점

2.2 VLAN

이런 문제점을 해결하기 위해 VLAN을 이용하여 네트워크의 노드들이 물리적인 위치와는 상관없이 다수의 노드들을 브로드캐스트 도메인으로 세그먼트하여 그룹을 구성함으로써 네트워크의 자원과 사용자들을 여러 작업 그룹으로 분리한다. 이렇게 함으로써 세그먼트간의 트래픽을 줄임은 물론 오직 인증된 사용자만이 이용할 수 있도록 하여 네트워크 보안을 향상시킨다. 이렇게 보안성을 향상시기 위해 VLAN 환경에서 구성하였지만 그 자체만으로 문제가 해결되는 것은 아니다. 왜냐하면 여전히 비인가된 사용자로부터의 접근을 차단할 수는 없다.

802.1Q 트렁킹은 원래의 이더넷 프레임의 발신지 주소 다음에 아래 (그림 2)와 같은 4바이트 길이의 802.1Q 태그를 추가하여 VLAN ID와 기타 정보를 표시한다.

802.1Q 프레임의 각 항목은 다음과 같은 의미를 가진다.



(그림 2) 802.3 이더넷 프레임/ IEEE 802.1Q 프레임

① Tag Protocol Identifier(VLAN Protocol ID, 2Bytes) : 0x8100의 고정된 값으로 현재 프레임이 802.1Q/802.1P프레임이라는 것을 표시한다.

② Tag Contorol Informaiton(TCI, 2Bytes) : 3비트 우선순위(Priority), 1비트 CFI(Cnanonicl Format Identifier), 12비트 VLAN 필드로 구성.

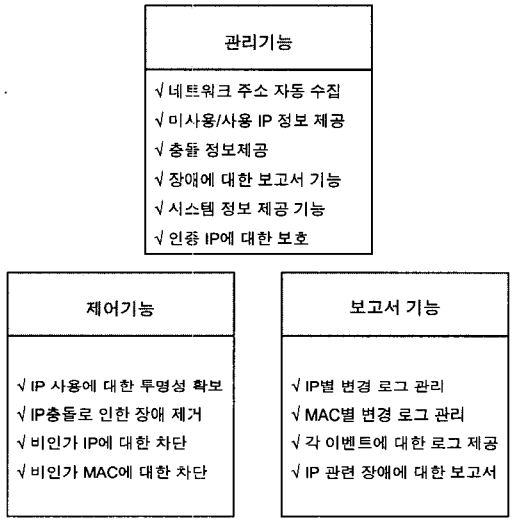
- 우선순위(Priority) : 프레임의 우선순위를 표시한다. 802.1p 우선순위 필드 또는, CoS (Class of Service)필드라고도 한다. 0에서 7사이값을 가지며, 값이 클수록 우선순위가 높다. 음성이나 동영상 데이터를 전송할 때 이 값을 크게 지정하여 우선순위를 높이고, 스위치에서 다른 프레임보다 빨리 처리되게 할 수 있다.
- CFI(Canonicla Format Indicator) : 인캡슐레이션된 프레임의 포맷이 Canonical 인지 아닌지를 구분한다. 0인 경우는 Canonical Format, 1인 경우는 Non canonical Format이다.
- VLAN Identifier(VID, 12bits) : 프레임의 VLAN 번호를 표시한다. 필드의 길이가 12비트이므로, 802.1Q 트렁킹 방식을 사용하면 0~4096개의 VLAN ID를 할당할 수 있다. 단, 우선순위 프레임을 식별하기 위한 0과 4095(FFF)는 예약된 주소로 사용할 수 없다. 구성 가능한 최대값은 4094이다.

3. 네트워크 주소 인증 모델 구성

실시간으로 네트워크를 효율적으로 관리하기 위해 네트워크 세그먼트 또는 VLAN(Virtual LAN) 단위로 네트워크에 사용되는 IP/MAC 주소현황을 모니터링 하는 기능을 제공하고 관리하는 시스템을 통해 정책기반으로 네트워크내의 시스템을 통제할 수 있는 기능을 제공한다.

네트워크 주소 인증 시스템은 크게 관리기능 제어 기능, 보고서 기능을 분류된다. (그림 3)은 각 기능별 세부 역할을 나타낸다.

위에서 언급하바와 같이 네트워크 주소 인증 시스템은 크게 두 가지 시스템으로 구성된다. 네트워크 주소 통합 관리 시스템과 네트워크 관리 에이전트 시스템이 그것이며 3.1과 3.2에서 각 시스템이 하고 있는 기능들에 대해서 기술하였다.



(그림 3) 인증 시스템의 주요 기능

3.1 네트워크 주소 통합 관리 시스템

관리 시스템은 현재 네트워크에서 사용되는 IP 주소 현황을 모니터링 하는 기능을 제공한다. 본 시스템을 사용하여 관리자는 에이전트 시스템으로부터 수집된 IP 주소 및 네트워크 자원 정보를 바탕으로 실시간으로 IP 주소 사용 현황을 확인할 수 있고, 비 인가된 사용자에 대해 IP 주소를 차단함으로써 보안 기능을 강화할 수 있다.

3.1.1 중앙 집중적 IP 주소 관리 기능

관리 시스템은 분산되어 있는 에이전트 시스

템들이 수집한 네트워크 정보 및 IP 주소를 수신 받는다. 이런 정보를 중앙에서 관리함으로써 IP 주소의 중복 사용을 피할 수 있고, 전체적인 IP 주소 사용 내역을 통계 낼 수 있다.

세부 기능	의 미
그룹 등록 관리	IP 주소별, 부서별, 층별로 사용자 그룹을 설정함으로써 실제 IP 주소 사용 여부 확인과 고정 IP 주소 및 MAC 주소에 대한 그룹별 사용 내역을 관리
상세 정보 관리	사용자 관리 목록을 통하여 특정 사용자나 장비에 대한 상세 정보 및 중요한 사항을 기록하여 관리하는 기능

3.1.2 IP 주소 사용 인증 관리 기능

관리자는 현재 사용중인 IP 주소를 관리 정책과 비교하여 정책에 위반되거나 비 인가된 사용자에 대해서는 IP 주소를 차단시킴으로써 네트워크 사용을 불가능하게 만들고 보안을 강화할 수 있다.

3.1.3 보고서 기능

네트워크에서 수집된 모든 정보는 정형화된 보고서 형태로 볼 수 있는 기능으로 분석하는 요청자의 관점에 따라 크게 총괄 보고서와 세부 보고서로 구분되어 진다.

세부 기능	의 미
총 괄 보고서	◦ 그룹별로 IP 주소 사용 내역에 대한 보고서를 관리자에게 제공 ◦ 관리자는 총괄 보고서를 바탕으로 개략적인 네트워크의 현 상태 및 장애에 대한 분석이 가능
상 세 보고서	◦ 로그파일에 대해 IP 주소별로 IP 주소 사용 내역에 대한 개별 보고서 ◦ 네트워크 내의 관리 대상들에 대한 명확하고 직관적인 보고서들을 제공

3.2 네트워크 주소 관리 에이전트

에이전트 시스템은 네트워크 세그먼트마다 설치되어 네트워크의 자원 정보 및 IP 주소를 수집하여 관리 시스템에게 통보하고 관리 시스템의 정책에 따라 IP 주소를 제어하는 시스템이다. 중앙 집중적인 관리 방식은 트래픽의 과부하를 발생시키기 때문에 분산적인 네트워크 환경에서는 에이전트 개념을 적용시킨 시스템 개발이 필요하다.

3.2.1 네트워크 자원 정보 자동 수집 기능

네트워크에 연결된 모든 자원인 IP 주소, MAC 주소, 시스템 이름, 사용자 이름을 자동으로 수집하는 기능이다. 수집된 정보는 관리 시스템에게 전달하고, 관리 시스템은 이 정보를 토대로 현재 사용중인 IP 주소 현황을 파악하고, 필요에 따라 IP 차단과 같은 제어 기능을 수행할 수 있다.

자원 정보	의 미
IP 주소	◦ 인터넷 상의 한 컴퓨터에서 다른 컴퓨터로 데이터를 보내는데 사용되는 프로토콜 ◦ 각 호스트마다 고유한 주소를 할당 ◦ IP 주소의 고유성은 보안 정책을 수행하는 데이터로 사용
MAC 주소	데이터 링크 계층의 MAC 계층에서 사용되는 고유한 주소로서 보안 정책을 수행하는 데이터로 사용

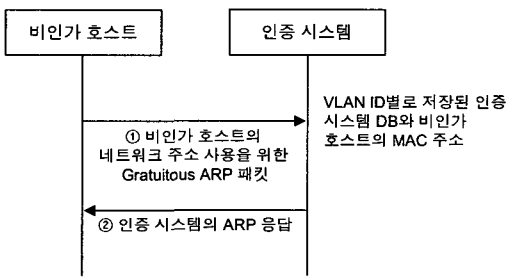
3.2.2 IP 주소 실시간 모니터링 기능

현재 네트워크에서의 브로드캐스트(broadcast) 패킷만을 실시간으로 모니터링 함으로써 네트워크 장비의 변경없이 네트워크 IP 주소 관리가 가능하다.

세부 기능	의 미
로그파일 저장	◦ 사용자별 실시간 특정 IP에 대해 MAC 및 사용자 명 변경 여부를 체계적으로 관리하여 내부 보안 사고에 대한 추적 가능 ◦ 사용자에서 발생된 실시간 이벤트 현황을 History 화하여 발생된 내부 문제점에 대해 빠른 조치가 가능
IP 주소 충돌 감지 기능	◦ 실시간으로 IP 주소의 충돌을 감지하고 이를 관리 시스템에게 TRAP 형식으로 알려주고 log를 기록 ◦ 관리자는 에이전트 시스템으로부터 통보된 IP 주소, MAC 주소, 시스템 이름, 사용자 이름 등의 TRAP 정보를 이용하여 네트워크의 장애를 신속히 해결
사용 기간 예약 및 제한	사용자별 내부 직원 및 외부 방문 사용자에 대해 IP를 사용할 수 있는 기간을 예약 설정하여 기간이 만료된 사용자에 대한 효율적인 관리를 제공

3.3 네트워크 주소 인증

IP 주소가 Static 혹은 DCHP 서버에 의해 할당될 경우 호스트는 네트워크에 접근할 권한을 가지게 된다. 물론 VLAN 환경일 경우 설정된 환경(포트기반, 맥기반)에 따라 제한된 네트워크 자원을 가진 호스트만이 네트워크를 사용하게 되지만 완벽히 비인가된 사용자로부터의 접근을 차단할 수는 없다. 하지만 다음에 제시된 방법을 통하여 네트워크 주소 인증을 통해 비인가된 사용자의 접근을 차단/통제 할 수 있다.

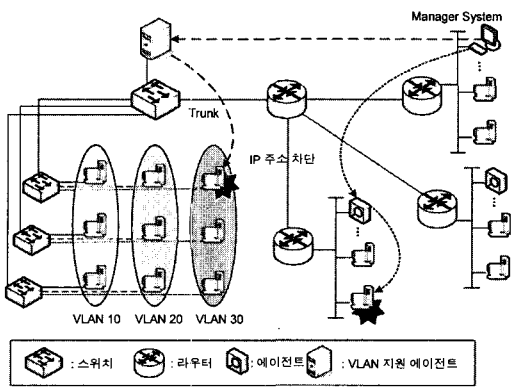


(그림 4) 네트워크 주소 인증 모델

(그림 4)는 비인가된 사용자가 네트워크에 접근하기 위해 초기에 자신이 사용하고자 하는 IP에 대해 Gratuitous ARP를 브로트캐스트로 전송한다. 이때 인증시스템은 자신이 VLAN 별로 저장하고 있는 정책을 기반으로 인증된 사용자임을 확인하고 만약 비인가된 사용자일 경우 ARP응답을 대신 보냄으로써 비인가된 사용자는 자신이 사용하고자하는 네트워크 주소를 사용할 수 없게 된다.

4. 정책 기반 인증 시스템 프레임 워크

(그림 5)에서 VLAN 환경을 지원하는 에이전트와 지원하지 않은 에이전트가 있다. 또한 매니저 시스템을 볼 수 있다. VLAN을 지원하는 에이전트는 모든 VLAN에서 전송하는 브로트캐스트 패킷을 모니터링 할 수 있게 트렁크 포트와 연결되어 있어야 한다. 매니저 시스템은 자동으로 수집된 정보를 토대로 VLAN 별로 한눈에 네트워크 주소사용을 알 수 있고 이를 토대로 정책을 설정하여 네트워크 자원을 관리할 수 있다. 만약 설정된 정책과 위배되는 행동을 하는 호스트가 네트워크에 접근시 이를 에이전트 시스템이 실시간으로 모니터링 차단/통제 후 이를 매니저 시스템에게 보고한다.



(그림 5) 네트워크 주소 인증 시스템 모델

본 시스템 도입 후 기대되는 활용 방안은 다음과 같다.

① IP/MAC 주소 사용에 대한 투명성 확보

IP/MAC 주소의 할당 시 인증 과정을 거치므로 어느 곳에서 어떠한 사용자가 사용하는지 파악할 수 있으며 이것은 장애 발생 시 어떠한 네트워크 요소로부터 장애가 발생하는지 파악하는데 상당한 도움을 줄 수 있다. 또한 다수의 IP를 사용하는 라우터, 스위치 및 DNS 서버 등의 네트워크 필수 장비에 대한 주소를 효과적으로 관리할 수 있다.

② IP 주소의 충돌로 인한 장애 발생 제거

IP 주소의 임의적 혹은 악의적 사용/변경으로 인해 발생할 수 있는 IP 주소 충돌 문제를 TCP/IP 네트워크의 기본적인 동작만으로 확인할수 있으며 이를 방지 할 수 있는 기술을 확보하여 네트워크 장애 요인을 사전에 제거할 수 있다.

③ 신속한 IP 할당을 위한 편리한 인터페이스

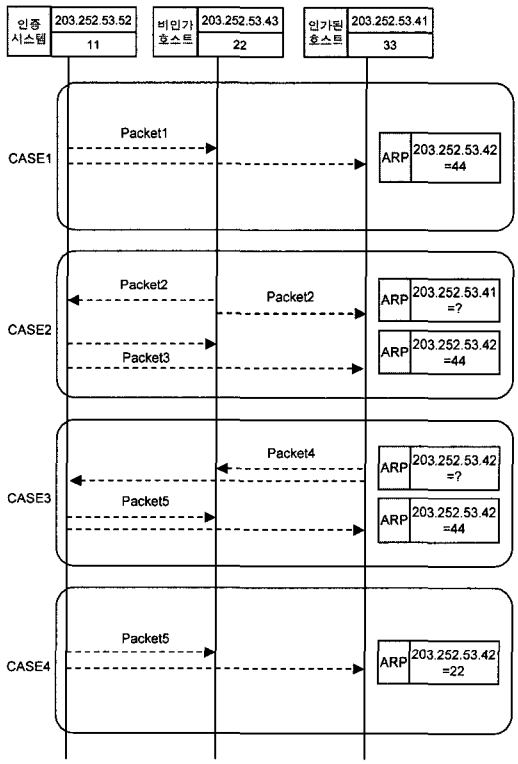
무선 네트워크를 이용하여 간헐적 혹은 임시로 IP를 할당 받아야 할 경우 관리자의 편의를 도모하기 위해 보다 가시적이고 직관적인 인터페이스를 제공함으로써 관리자는 각 상황에 신속하고 적절한 대응을 할 수 있다. 또한 본 시스템에 대한 관리자의 신속한 적응력을 갖출 수 있도록 한다.

④ 비인가 IP에 대한 사용을 사전에 차단

확보한 IP 주소에 대하여 인가된 IP만 사용할 수 있도록 사전에 조치함으로써 임의적 혹은 악의적 사용자로부터 인가되지 않은 IP를 사용하는 것을 사전에 방지 할 수 있다. 이것은 임의의 IP 주소를 이용하여 네트워크 자원을 낭비하거나 공격하는 등의 보안문제를 사전에 예방할 수 있다.

⑤ 네트워크 관리 시스템(NMS : Network Management System)과의 연동으로 장애에 대한 신속한 조치 가능

NMS에서 관리하는 자원에 대한 IP/MAC 주소를 함께 관리함으로써 IP 충돌로 인한 네트워크 장애를 사전에 방지하고 기타 장애 발생 시 NMS가 파악한 IP 주소를 이용하여 사용자의 정보를 탐색하여 장애 발생 요인을 쉽고 빠르게 대응할 수 있다.



(그림 6) 차단 및 통제 모델

(그림 6)에서 CASE 1의 경우는 비인가 호스트를 차단하기 위해서는 차단할 IP 주소에 대해 잘못된 MAC 주소를 연결하여 ARP 패킷을 생성 및 전송한다. 이때 사용되는 잘못된 MAC 주소는 에이전트 시스템의 MAC 주소를 사용하였

지만 호스트가 사용하지 않는 MAC 주소라면 다른 값이라도 무방하다. CASE2의 경우는 비인가된 호스트가 인가된 호스트에게 ARP 요청 패킷을 전송할 때이고 CASE 3은 인가된 호스트가 비인가된 호스트에게 ARP 요청 패킷을 전송할 때 이다. CASE 2, 3 두 가지 경우를 찾아내기 위해서 에이전트 시스템은 모든 ARP 패킷을 수집하며 Sender IP 주소 또는 Target IP 주소 부분에 차단된 호스트의 IP 주소가 있는지 검사한다. 만약 발견되었다면 즉시 잘못된 MAC 주소를 전송함으로서 차단을 유지한다. CASE 4는 차단 해제는 차단할 때와 마찬가지로 하나의 패킷만으로 이루어질 수 있다. 에이전트 시스템은 올바른 MAC 주소를 사전에 수집했기 때문에 차단 해제 메시지를 생성할 수 있다.

앞에서 언급한 4가지 경우에 대해 VLAN 환경일 경우 VLAN ID를 이더넷 프레임에 추가를 해야한다. 이 경우 자동으로 VLAN ID를 수집하기란 쉽지 않기 때문에 관리자가 수동으로 에이전트 시스템에 해당 VLAN ID를 입력해 주어야 한다.

5. 결 론

본 논문에서는 실시간으로 네트워크를 효율적으로 관리하기 위해 네트워크 세그먼트 또는 VLAN(Virtual LAN) 단위로 네트워크에 사용되는 IP/ MAC 주소현황을 모니터링 하는 기능을 제공하고 관리 시스템을 통해 정책기반으로 네트워크를 차단 및 통제 할 수 있는 기능에 대해 설명하였다. 각 브로드캐스트 도메인마다 에이전트를 설치하는 방식이 아닌, VLAN 트렁크 포트를 이용하여 필요한 에이전트의 개수를 줄이고 각 VLAN 별로 보안을 향상 시킬 수 있을 뿐만 아니라 네트워크 주소 인증을 통해 서로 다른 VLAN에 속해 있는 중요 자원으로 접근을 제한하는데 응용될 수 있다.

참 고 문 헌

[1] W. Richard Stevens, "TCP/IP Illustrated Volume 1", Addison Wesley, 1994.

[2] David C. Plummer, "An Ethernet Address Resolution Protocol", RFC 826.

[3] 권교혁, "Network Security Management Using ARP Spoofing", ICCSA LNCS, Vol. 3043, pp.142-149, 2004.

[4] Hastings, N. E., McLean, "TCP/IP spoofing fundamentals, Computers and Communications", *Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference*, pp.218-224.

[5] Ishibashi, H., Yamai, N., Abe, K., Matsuura, "A protection method against unauthorized access and address spoofing for open network access systems", *IEEE Pacific Rim Conference*, pp.10-13, 2001.

[6] Jain, S., Shenoy Ramam, D., Thirumalasetty, S. R., Saddi, M., Summa, "A Network Management Framework for Multi-layered Network: an Overview, Integrated Network Management Proceedings", *IEEE/IFIP International Symposium*, pp.14-18, 2001.

[7] IEEE standard for VLAN 802.1Q, 1998.

최 원 우

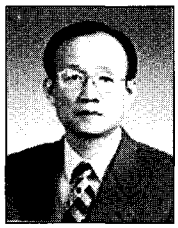
2003년 성균관대학교 정보공학과 (학사)

2003년~현재 성균관대학교 전기전자 및 컴퓨터공학부 대학원 석사과정

관심분야 : IPv6, 유무선 통합 네트워크, 네트워크 보안

안 성 진

1988년 성균관대학교 정보공학과 (학사)
1990년 성균관대학교 대학원 정보공학과(석사)
1990년~1995년 한국전자통신 연구원 연구전산망 개발실 연구원
1996년 정보통신 기술사 자격 취득
1998년 성균관대학교 대학원 정보공학과(박사)
2005년~현재 성균관대학교 컴퓨터교육과 부교수
관심분야 : 네트워크 관리, 트래픽 분석, Unix 네트워킹



정 진 욱

1974년 성균관대학교 전기공학과 학사
1979년 성균관대학교 대학원 전자공학과 석사
1991년 서울대학교 대학원 계산통계학과 박사
1982년~1985년 한국과학기술 연구소 실장
1981년~1982년 Racal Milgo Co. 객원연구원
1985년~현재 성균관대학교 전기전자 및 컴퓨터 공학부 교수
관심분야 : 컴퓨터 네트워크, 네트워크 관리, 네트워크 보안