

명세서

발명의 명칭: 네트워크에서의 접근 통제 시스템 및 그 방법

기술분야

- [1] 본 개시는 네트워크에서의 접근 통제 시스템 및 그 방법에 관한 것으로서, 더욱 상세하게는 서로 다른 세대에 위치하는 복수의 맥내 단말을 포함하는 네트워크서의 접근을 통제하기 위한 접근 통제 시스템 및 그 방법을 제공하는 것이다.

배경기술

- [2] 아파트 단지 내 각 세대에 설치되는 월 패드(Wall-Pad)에 다양한 기능들이 추가되고 있다. 월 패드에 카메라 등 다양한 기능이 탑재되면서, 최근 월 패드 해킹으로 인한 사생활 정보 유출이 사회적 문제로 대두하고 있다. 이에 따라, 아파트 단지 내 네트워크에서 서로 다른 세대의 월 패드로 접근하는 것을 통제하는 기능이 요구되고 있다. 또한, 월 패드와의 통신이 항상 허용되는 CCTV(closed circuit television), 주차관리 시스템 등의 주요 네트워크 장비를 통해 월 패드가 해킹 될 가능성 또한 존재하여, 이들 네트워크 장비를 IP(Internet Protocol) 주소/MAC(Media Access Control) 주소 도용 등의 해킹으로부터 보호해야 할 필요성도 대두되고 있다.
- [3] 통상적으로 아파트 단지 내 네트워크에서 같은 동의 월 패드들은 하나의 서브넷(Subnet)을 구성하며, 해당 서브넷 내 월 패드들 간에는 직접 통신 방식으로 통신이 이루어진다. 또한, 서로 다른 동의 월 패드들 간에도 서브넷 간의 통신을 통해 통신이 가능하다. 따라서, 월 패드를 해킹으로부터 보호하기 위해서는 아파트 단지 내 동일한 서브넷 내에서의 접근뿐만 아니라, 다른 서브넷에서의 접근도 통제될 필요가 있다.
- [4] 종래에는 아파트 단지 내 네트워크에서 월 패드 간 접근을 제어하기 위해, 스위치나 라우터 등 보안 장비에서 제공하는 ACL(Access Control List) 또는 방화벽(Firewall) 기능이 사용되었다. ACL 기술은 출발지 IP 주소, 목적지 IP 주소, 프로토콜, 어플리케이션 포트 번호 등으로 정의된 필터를 설정하고, 인-바운드(In-Bound) 또는 아웃-바운드(Out-Bound) 패킷에 대해 비교 검사를 실시하여, 해당 패킷을 허용하거나 차단하는 기술이다. ACL 기술은 화이트 리스트 또는 블랙리스트에 등록되지 않은 장비에 대해서는 패킷을 무조건 차단(Deny)하거나 통과시키도록 작동하여, 네트워크 구성 변경, 신규 장비 등록 등 네트워크 환경의 변화에 따른 정책 관리에 어려움이 발생한다. 또한, ACL 기술은 아파트 단지 내 서로 다른 동의 서브넷 간 통신은 차단이 가능하나, 같은 동 내의 월 패드 간 직접 통신은 차단이 어려울 수 있다. 하나의 서브넷에 속하는 같은 동 내 월 패드 간의 통신은 L3 스위치가 아닌 서브넷에 속한 L2 스위치를 통해 이루어진다. 따라서, L3 스위치에서 구성한 ACL 기능으로는 같은 동 내 월

패드 간 통신을 차단할 수 없다.

- [5] 또한, 아파트 단지 내 네트워크를 구성하는 서브넷 수 및 노드 수가 증가할수록, 즉 아파트의 동 수와 세대 수가 증가할수록, 월 패드 간 접근 제어를 위한 정책 관리가 복잡해지고, 이에 따른 장애 발생률 또한 증가하게 된다. 또한, 접근 제어 기능을 구성하기 위해 필요한 보안 장비의 수 또한 증가하여, 비용 증가, 보안 정책 가동률 감소 등의 문제가 발생할 수 있다.

발명의 상세한 설명

기술적 과제

- [6] 본 개시는 아파트 단지 내 세대별로 설치된 월 패드 등의 택내 단말에 대해 접근을 통제할 수 있는 접근 통제 시스템 및 그 방법을 제공하기 위한 것이다.

과제 해결 수단

- [7] 상기 과제를 해결하기 위한 일 실시 예에 따른 서로 다른 세대에 위치하는 복수의 택내 단말을 포함하는 네트워크에서의 접근 통제 방법은, 관리 장치가, ARP(Address Resolution Protocol) 요청 패킷들을 상기 복수의 택내 단말에 전송하는 단계, 상기 관리 장치가, 상기 ARP 요청 패킷에 대응하여 수신되는 제1 ARP 응답 패킷들을 분석하여 상기 복수의 택내 단말의 주소 정보를 획득하는 단계, 상기 관리 장치가, MAC(Media Access Control) 주소가 변조된 제2 ARP 응답 패킷들을 생성하는 단계, 그리고 상기 관리 장치가, 상기 제2 ARP 응답 패킷들을 상기 복수의 택내 단말에 전송함으로써, 상기 복수의 택내 단말의 ARP 테이블에서 각 택내 단말의 MAC 주소를 변조시키는 단계를 포함할 수 있다. 상기 제2 ARP 응답 패킷은, 각 ARP 테이블에서 MAC 주소를 변조하고자 하는 택내 단말의 IP 주소와 변조된 MAC 주소를 출발지 주소 정보로 포함하는 ARP 응답 패킷일 수 있다. 상기 변조된 MAC 주소는 통신이 불가능한 MAC 주소일 수 있다.
- [8] 상기 네트워크는, 서로 다른 네트워크 장치가 연결된 복수의 서브넷 각각에 대한 VLAN(Virtual Local Area Network) 대역 할당 정책 및 통신 허용 정책을 포함하는 액세스 관리 정책을 관리하는 정책 서버와, 상기 복수의 택내 단말을 포함하는 복수의 네트워크 장치를 포함할 수 있다. 상기 접근 통제 방법은, 상기 관리 장치가, 상기 복수의 네트워크 장치에 MAC 주소가 변조된 제3 ARP 응답 패킷을 전송하여, 상기 복수의 네트워크 장치의 ARP 테이블에서 게이트웨이의 MAC 주소를 상기 관리 장치의 MAC 주소로 변조시키는 단계, 상기 관리 장치가, 상기 복수의 네트워크 장치로부터 게이트웨이로 전송된 패킷을 수신하는 단계, 그리고, 상기 관리 장치가, 상기 액세스 관리 정책에 기초해 수신된 패킷을 상기 게이트웨이로 전달하거나 폐기하는 단계를 더 포함할 수 있다.
- [9] 상기 수신된 패킷을 상기 게이트웨이로 전달하거나 폐기하는 단계는, 상기 통신 허용 정책에서 상기 수신된 패킷의 목적지 IP 주소가 속한 VLAN 대역과 상기 수신된 패킷의 출발지 IP 주소가 속한 VLAN 대역 간의 통신이 금지된 경우,

상기 수신된 패킷을 폐기하는 단계를 포함할 수 있다.

- [10] 상기 수신된 패킷을 상기 게이트웨이로 전달하거나 폐기하는 단계는, 상기 통신 허용 정책에서 상기 수신된 패킷의 목적지 IP 주소가 속한 VLAN 대역과 상기 수신된 패킷의 출발지 IP 주소가 속한 VLAN 대역 간의 통신을 허용하는 경우, 상기 수신된 패킷을 상기 게이트웨이로 전달하는 단계를 포함할 수 있다.
- [11] 상기 수신된 패킷을 상기 게이트웨이로 전달하거나 폐기하는 단계는, 상기 수신된 패킷의 목적지 IP 주소가 상기 네트워크의 외부 네트워크에 속하면, 상기 수신된 패킷을 상기 게이트웨이에 전달하는 단계를 포함할 수 있다.
- [12] 상기 통신 허용 정책은, 상기 복수의 맥내 단말이 속한 서브넷들 간에는 통신이 금지되도록 설정될 수 있다.
- [13] 상기 접근 통제 방법은, 상기 관리 장치가, 상기 수신된 패킷으로부터 패킷을 전송한 네트워크 장치의 주소 정보를 획득하는 단계, 그리고 상기 관리 장치가, 상기 수신된 패킷으로부터 획득한 주소 정보와 상기 정책 서버에서 관리하는 주소 정보를 비교하여 신규 네트워크 장치를 검출하는 단계를 더 포함할 수 있다.
- [14] 상기 액세스 관리 정책은, 상기 신규 네트워크 장치의 인가 여부를 결정하기 위한 정책을 더 포함할 수 있다. 상기 접근 통제 방법은, 상기 정책 서버가, 상기 액세스 관리 정책 또는 관리자로부터 입력되는 제어 입력에 기초해 상기 신규 네트워크 장치의 인가 여부를 결정하는 단계, 그리고 상기 관리 장치가, 상기 신규 네트워크 장치가 비 인가된 장치이면, 상기 신규 네트워크 장치의 ARP 테이블에서 다른 네트워크 장치의 MAC 주소를 통신이 불가능한 MAC 주소로 변조하기 위한 제4 ARP 요청 패킷을 상기 신규 네트워크 장치에 전송하는 단계를 더 포함할 수 있다.
- [15] 상기 접근 통제 방법은, 상기 관리 장치가, 상기 신규 네트워크 장치가 비 인가된 장치이면, 상기 신규 네트워크 장치의 ARP 테이블에서 게이트웨이의 MAC 주소를 통신이 불가능한 MAC 주소 또는 상기 관리 장치의 MAC 주소로 변조하기 위한 제5 ARP 요청 패킷을 상기 신규 네트워크 장치에 전송하는 단계를 더 포함할 수 있다.
- [16] 상기 액세스 관리 정책은, 주소 도용 장치에 대한 차단 정책을 더 포함할 수 있다. 상기 접근 통제 방법은, 상기 관리 장치가, 상기 수신된 패킷으로부터 획득한 주소 정보와 상기 정책 서버에서 관리하는 주소 정보를 비교하여 상기 네트워크에 등록된 다른 네트워크 장치의 주소를 도용한 상기 주소 도용 장치를 검출하는 단계, 그리고 상기 관리 장치가, 상기 차단 정책에 기초해 상기 주소 도용 장치를 상기 네트워크로부터 차단하는 단계를 더 포함할 수 있다.
- [17] 상기 접근 통제 방법에서, 상기 관리 장치는, L3 스위치의 802.1Q 태그드 포트(802.1Q Tagged port)에 연결될 수 있다.
- [18] 또한, 일 실시 예에 따른 서로 다른 세대에 위치하는 복수의 맥내 단말을 포함하는 네트워크에서의 접근 통제 시스템은, ARP(Address Resolution Protocol)

요청 패킷들을 상기 복수의 맥내 단말에 전송하고, 상기 ARP 요청 패킷에 대응하여 수신되는 제1 ARP 응답 패킷들을 분석하여 상기 복수의 맥내 단말의 주소 정보를 획득하며, MAC(Media Access Control) 주소가 변조된 제2 ARP 응답 패킷들을 상기 복수의 맥내 단말에 전송함으로써, 상기 복수의 맥내 단말의 ARP 테이블에 등록된 각 맥내 단말의 MAC 주소를 변조시켜 상기 복수의 맥내 단말 간의 통신을 차단하는 관리 장치를 포함할 수 있다. 상기 제2 ARP 응답 패킷은, 각 ARP 테이블에서 MAC 주소를 변조하고자 하는 맥내 단말의 IP 주소와 변조된 MAC 주소를 출발지 주소 정보로 포함하는 ARP 응답 패킷일 수 있다. 상기 변조된 MAC 주소는 통신이 불가능한 MAC 주소일 수 있다.

- [19] 상기 접근 통제 시스템은, 상기 네트워크를 구성하는 복수의 서브넷 각각에 대한 VLAN(Virtual Local Area Network) 대역 할당 정책 및 통신 허용 정책을 포함하는 액세스 관리 정책을 관리하는 정책 서버를 더 포함할 수 있다. 상기 관리 장치는, 상기 네트워크에 등록된 복수의 네트워크 장치에 MAC 주소가 변조된 제3 ARP 응답 패킷을 전송하여 상기 복수의 네트워크 장치의 ARP 테이블에 등록된 게이트웨이의 MAC 주소를 상기 관리 장치의 MAC 주소로 변조시키고, 상기 복수의 네트워크 장치로부터 패킷이 수신되면 상기 액세스 관리 정책에 기초해 수신된 패킷을 상기 게이트웨이로 전달하거나 폐기하며, 상기 복수의 네트워크 장치는, 상기 복수의 맥내 단말을 포함할 수 있다.
- [20] 상기 관리 장치는, 상기 통신 허용 정책에서 상기 수신된 패킷의 목적지 IP 주소가 속한 VLAN 대역과 상기 수신된 패킷의 출발지 IP 주소가 속한 VLAN 대역 간의 통신이 금지된 경우, 상기 수신된 패킷을 폐기할 수 있다.
- [21] 상기 관리 장치는, 상기 통신 허용 정책에서 상기 수신된 패킷의 목적지 IP 주소가 속한 VLAN 대역과 상기 수신된 패킷의 출발지 IP 주소가 속한 VLAN 대역 간의 통신을 허용하거나, 상기 수신된 패킷의 목적지 IP 주소가 상기 네트워크의 외부 네트워크에 속하면, 상기 수신된 패킷을 상기 게이트웨이에 전달할 수 있다.
- [22] 상기 통신 허용 정책은, 상기 복수의 맥내 단말이 속한 서로 다른 서브넷 간에는 통신이 금지되도록 설정될 수 있다.
- [23] 상기 정책 서버는, 상기 복수의 네트워크 장치의 주소 정보를 관리하며, 상기 관리 장치는, 상기 수신된 패킷으로부터 패킷을 전송한 네트워크 장치의 주소 정보를 획득하고, 상기 수신된 패킷으로부터 획득한 주소 정보와 상기 정책 서버에서 관리하는 주소 정보를 비교하여 신규 네트워크 장치를 검출할 수 있다.
- [24] 상기 액세스 관리 정책은, 상기 신규 네트워크 장치의 인가 여부를 결정하기 위한 정책을 더 포함할 수 있다. 상기 정책 서버는, 상기 액세스 관리 정책 또는 관리자로부터 입력되는 제어 입력에 기초해 상기 신규 네트워크 장치의 인가 여부를 결정할 수 있다. 상기 관리 장치는, 상기 신규 네트워크 장치가 비 인가된 장치이면, 상기 신규 네트워크 장치의 ARP 테이블에서 다른 네트워크 장치의 MAC 주소를 통신이 불가능한 MAC 주소로 변조하기 위한 제4 ARP 요청 패킷을

상기 신규 네트워크 장치에 전송할 수 있다.

- [25] 상기 관리 장치는, 상기 신규 네트워크 장치가 비 인가된 장치이면, 상기 신규 네트워크 장치의 ARP 테이블에서 게이트웨이의 MAC 주소를 통신이 불가능한 MAC 주소 또는 상기 관리 장치의 MAC 주소로 변조하기 위한 제5 ARP 요청 패킷을 상기 신규 네트워크 장치에 전송할 수 있다.

- [26] 상기 액세스 관리 정책은, 주소 도용 장치에 대한 차단 정책을 더 포함할 수 있다. 상기 관리 장치는, 상기 수신된 패킷으로부터 획득한 주소 정보와 상기 정책 서버에서 관리하는 주소 정보를 비교하여 상기 네트워크에 등록된 다른 네트워크 장치의 주소를 도용한 상기 주소 도용 장치를 검출하며, 상기 차단 정책에 기초해 상기 주소 도용 장치를 상기 네트워크로부터 차단할 수 있다.

- [27] 상기 관리 장치는, L3 스위치의 802.1Q 태그드 포트(802.1Q Tagged port)에 연결될 수 있다.

발명의 효과

- [28] 본 개시에 따르면 아파트 단지 내 세대별로 설치된 월 패드 등의 벽내 단말에 대한 불법적인 접근을 효과적으로 차단할 수 있다.

도면의 간단한 설명

- [29] 도 1은 일 실시 예에 따른 아파트 단지 내 네트워크를 개략적으로 도시한다.
[30] 도 2는 일 실시 예에 따른 접근 통제 시스템을 개략적으로 도시한다.
[31] 도 3은 일 실시 예에 따른 네트워크에서의 접근 통제 방법을 개략적으로 도시한다.
[32] 도 4는 일 실시 예에 따른 네트워크에서 주소 도용 장치의 접근을 차단하는 방법을 개략적으로 도시한다.

발명의 실시를 위한 형태

- [33] 이하, 첨부된 도면을 참조하여 본 명세서에 개시된 실시 예를 상세히 설명하되, 동일하거나 유사한 구성요소에는 동일, 유사한 도면 부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 이하의 설명에서 사용되는 구성요소에 대한 접미사 "모듈" 및 "부"는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서, 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다. 또한, 본 명세서에 개시된 실시 예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시 예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시 예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않으며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.
- [34] 제1, 제2 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 구성요소들은 이 용어들에 의해 한정되지는 않는다. 용어들은

하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

- [35] 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.
- [36] 본 출원에서, "포함한다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [37] 도 1은 일 실시 예에 따른 아파트 단지 내 네트워크를 개략적으로 도시한다.
- [38] 도 1을 참조하면, 아파트 단지 내 네트워크(1)에서 외부 네트워크(인터넷)와 송수신 되는 패킷들은 방화벽(11) 및 L3 스위치(12)를 통과한다. 방화벽(11)은 네트워크(1)의 보안을 담당하며, 네트워크 내부로 들어오거나 외부로 나가는 유해 트래픽을 차단하는 기능을 수행할 수 있다. L3 스위치(12)는 네트워크(1)에서 인터넷에 연결하고자 하는 노드들의 중심에 위치하는 백본 스위치(backbone switch)로 작동할 수 있다. 이 경우, 네트워크(1)와 인터넷 사이에 송수신 되는 모든 패킷들이 L3 스위치(12)를 통과하게 된다. L3 스위치(12)는 네트워크(1)의 게이트웨이(gateway)로서 작동할 수도 있다. 게이트웨이는 각 패킷에 포함된 목적지 IP 주소에 기초해, 인터넷과 네트워크(1) 사이, 또는 네트워크(1)를 구성하는 서브넷들 사이에서 패킷을 전달할 수 있다.
- [39] 네트워크(1)는 적어도 하나의 서브넷(subnet)(20)을 포함할 수 있다.
- [40] 아파트 단지 내 네트워크(1)에서 각 서브넷(20)은 같은 동에 위치하는 택내 단말(22)들 및 이들 사이의 통신을 지원하는 적어도 하나의 L2 스위치(21)를 포함할 수 있다. 동일한 서브넷(20)에 속하는 택내 단말(22)들 즉, 같은 동에 속하는 택내 단말(22)들 간의 통신은 L2 스위치(21)를 통한 직접 통신에 해당할 수 있다. 서로 다른 서브넷(20)에 속하는 택내 단말(22)들 즉, 서로 다른 동에 속하는 택내 단말(22)들 간의 통신은 L3 스위치(12)의 게이트웨이를 통한 서브넷(20) 간 통신에 해당할 수 있다. 택내 단말(22)은 각 세대 내에 위치하는 네트워크 장치로서, 아파트 단지/세대 내 정보 제공 기능, 아파트 단지/세대 내 설비 제어 기능, 통화 기능 등 다양한 기능을 수행할 수 있다. 택내 단말(22)은 예를 들어, 비디오 폰, 도어 폰, 월패드 등을 포함할 수 있다.
- [41] 네트워크(1)는 택내 단말(22) 외에도 아파트 단지 내에서 네트워크(1)를 통해 관리되는 각종 공용 시스템(예를 들어, CCTV(31), 주차관리 시스템(32), 단지 출입문(33), 공동 현관문(34) 등)을 포함할 수 있다. 네트워크(1)는 단지 서버(41), 통화 서버(42) 등 아파트 단지 내 위치하는 각종 서버를 더 포함할 수 있다.
- [42] 네트워크(1)에서, 공용 시스템들(예를 들어, CCTV(31), 주차관리 시스템(32), 단지 출입문(33), 공동 현관문(34) 등)과 각종 서버들(예를 들어, 단지 서버(41), 통화 서버(42) 등)은 적어도 하나의 서브넷(30, 40)을 구성할 수 있다. 네트워크(1)에서 각 서브넷(20, 30, 40)은 가상 랜(Virtual Local Area Network,

VLAN) 대역으로 구분될 수 있다. 즉, 서브넷들(20, 30, 40)에는 서로 다른 VLAN 대역이 할당될 수 있다.

- [43] 아래에서는, 설명의 편의를 위해, 네트워크(1)에 속하는 맥내 단말(22), 공용 시스템(CCTV(31), 주차관리 시스템(32), 단지 출입문(33), 공동 현관문(34) 등), 및 서버(단지 서버(41), 통화 서버(42) 등)를 '네트워크 장치'로 통칭할 수도 있다.
- [44] 네트워크(1)는 네트워크(1)에 속하는 네트워크 장치에 대한 불법적인 접근을 차단하기 위해 정책 서버(43) 및 관리 장치(13)를 더 포함할 수 있다.
- [45] 도 2는 일 실시 예에 따른 아파트 단지 내 네트워크(1)에서 네트워크 장치에 대한 접근을 통제하기 위한 접근 통제 시스템을 개략적으로 도시한다.
- [46] 도 2를 참조하면, 접근 통제 시스템(100)은 전술한 도 1의 L3 스위치(12), 관리 장치(13) 및 정책 서버(43)를 포함할 수 있다.
- [47] 관리 장치(13) 및 정책 서버(43)는 L3 스위치(12)에 연결되며, L3 스위치(12)를 통해 서로 통신할 수 있다.
- [48] 정책 서버(43)는 네트워크(1)에서 네트워크 액세스에 대한 정책(액세스 관리 정책) 및 네트워크 장치들의 장치 정보를 설정하고 관리하는 기능을 수행할 수 있다.
- [49] 정책 서버(43)는 데이터베이스(431) 및 정책 관리부(432)를 포함할 수 있다.
- [50] 데이터베이스(431)는 네트워크(1)에서의 네트워크 액세스에 대한 연결 인증, 권한 부여, 계정 작업 등을 위한 정책(액세스 관리 정책) 정보를 저장할 수 있다. 액세스 관리 정책은, 네트워크(1)를 구성하는 각 서브넷(20, 30, 40)에 대한, VLAN 대역(또는 서브넷 대역) 할당 정책, 통신 허용 정책(각 VLAN 대역에 대한 통신 허용 정책, VLAN 대역 간의 통신 허용 정책)을 포함할 수 있다. 예를 들어, 통신 허용 정책은, 맥내 단말(22)들이 속한 서로 다른 서브넷(20) 간에는 통신이 차단되고, 맥내 단말(22)들이 속하는 서브넷(20)과 주차관리 시스템(32)이 속한 서브넷(30) 간에는 통신이 가능하도록 설정될 수 있다. 액세스 관리 정책은 네트워크(1)에 새로이 접속을 시도하는 네트워크 장치의 인가 여부를 결정하기 위한 정책, 네트워크(1)에 의해 비인가 되거나, 다른 네트워크 장치의 주소를 도용한 장치에 대한 차단 정책 등을 더 포함할 수 있다.
- [51] 데이터베이스(431)는 네트워크(1)에 등록된 각 네트워크 장치의 장치 정보를 더 포함할 수 있다. 장치 정보는, 각 네트워크 장치의 주소 정보(IP 주소 및 MAC 주소), 상태 정보(온라인/오프라인), 인증 정보(인가/비인가), 차단 여부 등을 포함할 수 있다.
- [52] 정책 관리부(432)는 데이터베이스(431)에 저장되는 정책 정보를 설정 및 관리할 수 있다. 정책 관리부(432)는 관리자로부터 수신되는 제어 입력에 기초해 정책 정보를 설정 및 관리할 수 있다.
- [53] 정책 관리부(432)는 데이터베이스(431)에 저장되는 장치 정보를 설정 및 관리할 수도 있다. 정책 관리부(432)는 관리 장치(13)로부터 각 네트워크 장치의 주소 정보, 상태 정보 등을 수신하고, 수신된 정보들에 기초해 장치 정보를 설정

및 관리할 수 있다.

- [54] 정책 관리부(432)는 관리 장치(13)로부터 신규 네트워크 장치의 검출이 통지되면, 관리 장치(13)로부터 수신되는 신규 네트워크 장치의 정보에 기초해 신규 네트워크 장치의 인가 여부를 결정할 수 있다. 정책 관리부(432)는 데이터베이스(431)에 저장된 정책 정보에 기초해 신규 네트워크 장치의 인가 여부를 결정할 수 있다. 정책 관리부(432)는 신규 네트워크 장치의 검출을 관리자에게 통지하고, 이후 관리자로부터 수신되는 제어 입력에 기초해 해당 네트워크 장치의 인가 여부를 결정할 수도 있다.
- [55] 정책 관리부(432)는 또한 신규 네트워크 장치에 대한 인가 여부가 결정되면, 대응하는 인가 정보를 관리 장치(13)에 전송할 수도 있다.
- [56] 관리 장치(13)는 ARP(Address Resolution Protocol) 패킷 변조 및 패킷 포워딩을 사용해 네트워크(1)에 대한 접근을 통제할 수 있다.
- [57] 관리 장치(13)는 저장부(131), 송수신부(132), 및 제어부(133)를 포함할 수 있다.
- [58] 저장부(131)는 관리 장치(13)에서 처리되는 각종 정보, 데이터 등을 저장할 수 있다. 저장부(131)는 정책 서버(43)로부터 수신되는 정보(정책 정보, 장치 정보 등)를 저장할 수 있다. 저장부(131)는 후술하는 제어부(133)에 의해 획득되는 각 네트워크 장치의 주소 정보, 상태 정보 등을 저장할 수도 있다. 저장부(131)는 송수신부(132)를 통해 송수신되는 패킷들을 임시 저장할 수도 있다.
- [59] 송수신부(132)는 네트워크(1)에 속한 다른 장치와 관리 장치(13) 사이에서 정보, 패킷 등을 송수신할 수 있다.
- [60] 송수신부(132)는 정책 서버(43)로부터 정책 정보, 장치 정보 등을 수신할 수 있다. 송수신부(132)는 정책 서버(43)에 이벤트 발생을 통지하고, 관리 장치(13)에 의해 획득된 네트워크 장치의 상태 정보, 주소 정보 등을 정책 서버(43)에 전송할 수도 있다.
- [61] 송수신부(132)는 네트워크(1) 내에서 L3 스위치(12)를 통해 전달되는 패킷들(ARP 패킷, UDP(User Datagram Protocol) 패킷, TCP(Transmission Control Protocol) 패킷 등)을 수집할 수 있다. 송수신부(132)는 L3 스위치(12)의 802.1Q 태그드 포트(802.1Q Tagged port)(또는 트렁크 포트(trunk port))에 연결될 수 있다. L3 스위치(12)의 802.1Q 태그드 포트는, 다수의 VLAN 대역 트래픽이 통과하는 포트이다. 위에서 설명한 바와 같이, 네트워크(1)의 각 서브넷(20, 30, 40)에는 서로 다른 VLAN 대역이 할당될 수 있다. 따라서, 관리 장치(13)가 L3 스위치(12)를 통해 전달되는 모든 서브넷(20, 30, 40)의 패킷들을 수집하기 위해서는, 서브넷(20, 30, 40)들에 할당된 모든 VLAN 대역에 접근할 수 있어야 하며, 이를 위해 송수신부(132)는 L3 스위치(12)의 802.1Q 태그드 포트에 연결될 수 있다.
- [62] 송수신부(132)는 네트워크(1)에 접속하는 각 네트워크 장치(예를 들어, 맥내 단말(22))와 ARP 패킷(ARP 요청(request) 패킷, ARP 응답(response) 패킷 등)을 송수신할 수도 있다.

- [63] 송수신부(132)는 다른 네트워크 장치로부터 수신한 패킷을 게이트웨이(예를 들어, 게이트웨이 기능을 수행하는 L3 스위치(12))로 포워딩(forwarding)할 수도 있다.
- [64] 제어부(133)는 관리 장치(13)의 전반적인 작동을 제어할 수 있다.
- [65] 제어부(133)는 관리 장치(13)의 작동이 개시되면, 정책 서버(43)로부터 정책 정보, 네트워크 장치들의 장치 정보 등을 수신하여, 저장부(131)에 저장할 수 있다.
- [66] 또한, 제어부(133)는 각 VLAN 대역(서브넷 대역) 별로 ARP 요청 패킷을 전송하여, 각 VLAN 대역(서브넷 대역)에 연결된 네트워크 장치들의 정보(주소 정보, 상태 정보 등)를 획득할 수 있다.
- [67] 제어부(133)는 정보를 확인하고자 하는 네트워크 장치의 IP 주소를 목적지 주소 정보로 포함하는 ARP 요청 패킷을 해당 네트워크 장치가 속한 서브넷으로 브로드캐스팅할 수 있다. 그런 다음, 제어부(133)는 전송된 ARP 요청 패킷에 대한 ARP 응답 패킷이 수신되는지 여부에 기초하여 대응하는 네트워크 장치의 상태 정보를 결정할 수 있다. 즉, 제어부(133)는 소정 시간 동안 ARP 요청 패킷을 적어도 1회 이상 전송한 후, 대응하는 네트워크 장치로부터 소정 시간 내에 ARP 응답 패킷이 수신되지 않은 경우, 해당 네트워크 장치가 오프라인 상태인 것으로 판단할 수 있다. 제어부(133)는 ARP 요청 패킷을 전송한 후 소정 시간 내에 대응하는 네트워크 장치로부터 ARP 응답 패킷이 수신되면, 해당 네트워크 장치가 온라인 상태인 것으로 판단할 수 있다. 제어부(133)는 각 네트워크 장치의 상태가 온라인 또는 오프라인으로 결정되면, 결정된 상태를 토대로 각 네트워크 장치의 상태 정보를 설정하고, 이를 저장부(131)에 저장할 수 있다. 여기서, 온라인 상태는 해당 네트워크 장치와 네트워크(1) 간의 연결이 활성화된 상태를 나타내고, 오프라인 상태는 해당 네트워크 장치와 네트워크(1) 간의 연결이 비활성화된 상태를 나타낼 수 있다.
- [68] 제어부(133)는 상태 정보가 획득되면, 이를 해당 네트워크 장치의 이전 상태 정보와 비교하여 상태 변경 이벤트를 검출할 수도 있다. 여기서, 해당 네트워크 장치의 이전 상태 정보는, 정책 서버(43)로부터 수신한 해당 네트워크 장치의 장치 정보, 또는 저장부(131)에 저장된 해당 네트워크 장치의 이전 상태 정보로부터 획득할 수 있다. 제어부(133)는 오프라인 상태에서 온라인 상태, 또는 온라인 상태에서 오프라인 상태로 상태가 변경된 네트워크 장치가 검출되면, 해당 네트워크 장치에 대해 상태 변경 이벤트가 발생한 것으로 결정할 수 있다. 제어부(133)는 적어도 하나의 네트워크 장치에서 상태 변경 이벤트 발생이 검출되면, 상태 변경 이벤트 발생을 정책 서버(43)에 통지할 수 있다. 또한, 제어부(133)는 정책 서버(43)에 저장된 장치 정보를 업데이트하도록 업데이트된 상태 정보를 정책 서버(43)에 전달할 수 있다.
- [69] 제어부(133)는 ARP 요청 패킷을 네트워크 장치들에 전송한 후 이에 대한 ARP 응답 패킷이 수신되면, 수신된 ARP 응답 패킷을 분석하여 각 네트워크 장치의

주소 정보(IP 주소 및 MAC 주소)를 획득할 수도 있다. 관리 장치(13)로부터 전송된 ARP 요청 패킷의 목적지 주소 정보로부터 자신의 IP 주소를 확인한 네트워크 장치는, 자신의 IP 주소 및 MAC 주소를 출발지 주소 정보로 포함하는 ARP 응답 패킷을 전송할 수 있다. 따라서, 제어부(133)는 ARP 응답 패킷이 수신되면, 해당 응답 패킷에 포함된 출발지 주소 정보(출발지 IP 주소 및 출발지 MAC 주소)로부터 대응하는 네트워크 장치의 주소 정보(IP 주소 및 MAC 주소)를 획득할 수 있다.

- [70] 제어부(133)는 전술한 방식으로 아파트 단지 내 각 세대에 설치된 택내 단말(22)들의 상태 정보 및 주소 정보를 수집할 수 있으며, 각 택내 단말(22)이 어느 서브넷(20)(VLAN 대역)에 속하는지 또한 확인할 수 있다.
- [71] 제어부(133)는 전술한 방식으로 수집된 정보들에 기초해 각 서브넷(20)에 연결된 택내 단말(22)들을 식별하고, ARP 패킷 변조를 사용해 동일한 서브넷(20)에 속하는 서로 다른 세대의 택내 단말(22)간의 통신을 차단할 수 있다.
- [72] 제어부(133)는 각 택내 단말(22)의 주소 정보에 기초해, 각 택내 단말(22)의 ARP 테이블에서 MAC 주소들을 변조시키기 위한 변조된 ARP 응답 패킷들을 생성할 수 있다. 각각의 변조된 ARP 응답 패킷은, MAC 주소 변조 대상인 택내 단말(22)의 IP 주소와 변조된 MAC 주소를 출발지 주소 정보로 포함할 수 있다. 변조된 MAC 주소는 통신에 부적합한 의미 없는 MAC 주소일 수 있다.
- [73] 제어부(133)는 변조된 ARP 응답 패킷이 생성되면, 이를 MAC 주소 변조 대상인 택내 단말(22)이 속한 서브넷(20)으로 전송할 수 있다. 이에 따라, 변조된 ARP 응답 패킷을 수신하게 된 같은 서브넷(20)의 다른 택내 단말(22)들은 수신된 ARP 응답 패킷에 포함된 출발지 주소 정보에 기초해 자신에 저장된 ARP 테이블을 업데이트할 수 있다. 즉, 변조된 ARP 응답 패킷을 수신한 각 택내 단말(22)은, 수신된 ARP 응답 패킷으로부터 출발지 IP 주소 및 출발지 MAC 주소를 획득하고, 자신의 ARP 테이블에서 출발지 IP 주소에 대응하는 MAC 주소를 출발지 MAC 주소로 변경할 수 있다.
- [74] 각 네트워크 장치의 ARP 테이블은, 해당 네트워크 장치와 동일한 브로드캐스트 도메인(예를 들어, 서브넷)에 속한 네트워크 장치들의 주소 정보(IP 주소 및 MAC 주소)와 해당 네트워크 장치가 연결되는 게이트웨이의 주소 정보(IP 주소 및 MAC 주소)를 포함할 수 있다. 각 택내 단말(22)은 동일한 서브넷(20)에 속한 다른 택내 단말(22)과 통신하기 위해 이 ARP 테이블에 저장된 상대측 택내 단말(22)의 주소 정보를 참조한다. 따라서, 동일한 서브넷(20)에 속한 택내 단말(22)들이 다른 택내 단말(22)과 통신하기 위해 참조하는 ARP 테이블의 MAC 주소들을 통신이 불가능한 MAC 주소로 변조시킬 경우, 택내 단말(22)은 같은 서브넷(20)에 속한 다른 택내 단말(22)의 올바른 MAC 주소를 알 수 없어 다른 택내 단말(22)과의 직접 통신이 불가능하게 된다.
- [75] 제어부(133)는 ARP 패킷 변조 및 패킷 포워딩(forwarding)을 사용해 서로 다른

서브넷에 속한 네트워크 장치 사이의 접근을 통제할 수도 있다.

- [76] 제어부(133)는 접근 통제가 필요한 각 서브넷에 대해 게이트웨이(예를 들어, L3 스위치(12))의 MAC 주소를 관리 장치(13)의 MAC 주소로 변조하기 위해 변조된 ARP 응답 패킷을 생성하고, 변조된 ARP 응답 패킷을 각 서브넷에 전송할 수 있다. 변조된 ARP 응답 패킷은, 게이트웨이(L3 스위치(12))의 IP 주소와 관리 장치(13)의 MAC 주소를 출발지 주소 정보로 포함할 수 있다. 이를 수신한 각 네트워크 장치는 자신에 저장된 ARP 테이블에서 게이트웨이의 MAC 주소를 관리 장치(13)의 MAC 주소로 업데이트할 수 있다. 이에 따라, 특정 네트워크 장치가 자신이 속한 서브넷의 외부(다른 서브넷 또는 네트워크(1)의 외부 네트워크)로 향하는 패킷을 전송하면, 이는 L3 스위치(12)의 게이트웨이가 아닌 관리 장치(13)로 전달될 수 있다. 즉, 제어부(133)는 각 네트워크 장치가 자신이 속한 서브넷의 외부(인터넷 또는 다른 서브넷)로 패킷을 전송하면, 전송된 패킷을 게이트웨이 대신 수신할 수 있다.
- [77] 제어부(133)는 게이트웨이 대신 패킷을 수신하면, 수신된 패킷의 출발지 IP 주소 및 목적지 IP 주소에 기초해 수신된 패킷의 출발지 서브넷과 목적지 서브넷을 확인할 수 있다. 또한, 제어부(133)는 정책 서버(43)로부터 수신한 정책 정보(VLAN 대역(또는 서브넷 대역) 간의 통신 허용 정책)에 기초해, 출발지 서브넷에서 목적지 서브넷으로의 접근이 허용된 상태인지를 확인할 수 있다. 제어부(133)는 통신 허용 정책에서 출발지 서브넷에서 목적지 서브넷으로의 접근이 금지된 상태이면, 해당 패킷을 포워딩 하지 않고 폐기하여 접근을 차단할 수 있다. 예를 들어, 맥내 단말(22)이 다른 동(다른 서브넷(20))에 속한 맥내 단말(22)에 접속하기 위해 패킷을 전송한 경우가 이 경우에 해당하며, 이 경우 맥내 단말(22)로부터 전송된 패킷은 폐기되어 전달이 차단될 수 있다. 제어부(133)는 통신 허용 정책에서 출발지 서브넷에서 목적지 서브넷으로의 접근이 허용된 상태이면, 해당 패킷이 목적지에 정상적으로 전달되도록 해당 패킷을 게이트웨이(L3 스위치(12))로 포워딩 할 수 있다. 예를 들어, 맥내 단말(22)이 아파트 단지 내 공통으로 사용되는 네트워크 장치(예를 들어, CCTV(31), 주차관리 시스템(32), 단지 출입문(33), 공동 현관문(34) 등)에 접속하기 위해 패킷을 전송한 경우가 이 경우에 해당하며, 이 경우 맥내 단말(22)로부터 전송된 패킷은 목적지에 정상적으로 전달하기 위해 게이트웨이로 포워딩 된다.
- [78] 제어부(133)는 수신된 패킷이 네트워크(1)의 외부 네트워크로 전송되는 패킷인 경우에도, 해당 패킷이 정상적으로 전달되도록 게이트웨이(L3 스위치(12))로 포워딩 할 수 있다.
- [79] 게이트웨이(L3 스위치(12))는 관리 장치(13)로부터 패킷이 포워딩 되면, 포워딩된 패킷의 목적지 주소를 확인하여 해당 패킷을 목적지인 서브넷 또는 외부 네트워크로 전송할 수 있다.
- [80] 제어부(133)는 네트워크 장치들로부터 수신되는 패킷들을 지속적으로

분석하여 각 네트워크 장치의 상태 정보를 업데이트할 수 있다. 제어부(133)는 패킷이 수신되면, 수신된 패킷의 출발지 주소 정보에 기초해 해당 패킷을 전송한 네트워크 장치가 정책 서버(43)에 이미 등록된 네트워크 장치인지 확인할 수 있다. 제어부(133)는 패킷을 전송한 네트워크 장치가 이미 등록된 네트워크 장치이면 해당 네트워크 장치가 온라인 상태인 것으로 확인할 수 있다. 또한, 제어부(133)는 정책 서버(43)에 등록된 네트워크 장치들(즉, 정책 서버(43)의 장치 정보에 주소 정보가 등록된 네트워크 장치들) 중 소정 시간 동안 패킷을 전송하지 않은 네트워크 장치가 확인되면, 전송한 바와 같이 ARP 패킷을 사용해 해당 네트워크 장치의 상태를 확인할 수 있다. 즉, 제어부(133)는 해당 네트워크 장치의 상태 확인을 위한 ARP 요청 패킷을 전송하고, 이에 대한 ARP 응답 패킷의 수신 여부에 기초해 해당 네트워크 장치의 상태를 확인할 수 있다.

- [81] 제어부(133)는 네트워크 장치들로부터 수신되는 패킷들을 지속적으로 분석하여 네트워크(1)에 새로 접속을 시도하는 신규 네트워크 장치를 검출할 수도 있다. 제어부(133)는 네트워크 장치로부터 패킷이 수신되면, 수신된 패킷으로부터 출발지 주소 정보(출발지 IP 주소 및 출발지 MAC 주소)를 획득하고, 이를 기 등록된 네트워크 장치들의 주소 정보와 비교하여 해당 패킷을 전송한 네트워크 장치가 신규 장치인지를 확인할 수 있다. 제어부(133)는 기 등록된 네트워크 장치들의 주소 정보 중에서, 수신된 패킷으로부터 획득한 출발지 주소 정보와 동일한 주소 정보가 검색되지 않으면, 해당 패킷을 전송한 네트워크 장치가 네트워크(1)에 새로 연결된 신규 장치인 것으로 판단할 수 있다. 제어부(133)는 패킷을 전송한 네트워크 장치가 신규 장치인 것으로 확인되면, 정책 서버(43)에 신규 장치 검출 이벤트 발생을 통지하고, 해당 네트워크 장치의 주소 정보(IP 주소 및 MAC 주소)를 정책 서버(43)에 전송할 수도 있다.
- [82] 정책 서버(43)는 관리 장치(13)로부터 신규 네트워크 장치의 검출이 통지되면, 액세스 관리 정책 또는 관리자로부터 수신되는 제어 입력에 기초해 신규 네트워크 장치에 대한 인가 여부를 결정할 수 있다. 정책 서버(43)는 신규 네트워크 장치가 인가되면, 신규 네트워크 장치를 네트워크(1)에 등록하고 신규 네트워크 장치의 주소 정보를 데이터베이스(431) 내 장치 정보에 포함시킬 수 있다. 또한, 정책 서버(43)는 신규 네트워크 장치의 인가 유무를 나타내는 정보를 관리 장치(13)에 전송할 수 있다.
- [83] 제어부(133)는 신규 네트워크 장치에 대한 인가 정보(인가/비인가)를 정책 서버(43)로부터 수신하면, 신규 네트워크 장치의 인가 여부에 따라서 네트워크(1)에 대한 신규 네트워크 장치의 접근을 차단할 수 있다. 제어부(133)는 신규 네트워크 장치가 비 인가된 장치인 경우, 변조된 ARP 응답 패킷을 사용하여 비 인가된 네트워크 장치의 ARP 테이블에서 비 인가된 네트워크 장치와 동일한 서브넷에 속하는 네트워크 장치들의 MAC 주소를 통신이 불가능한 의미 없는 MAC 주소로 변조할 수 있다. 즉, 제어부(133)는 비 인가된 네트워크 장치와 동일한 서브넷에 속하는 각 네트워크 장치의 MAC 주소를 의미 없는 주소로

변조하기 위한 변조된 ARP 응답 패킷을 생성하고, 이를 비 인가된 네트워크 장치가 속한 서브넷으로 전송할 수 있다. 이를 수신한 비 인가된 네트워크 장치는, 변조된 ARP 응답 패킷으로부터 획득한 주소 정보에 기초해 자신의 ARP 테이블을 업데이트하고, 이로 인해 비 인가된 네트워크 장치가 해당 네트워크 장치의 올바른 MAC 주소를 확인할 수 없게 된다.

- [84] 제어부(133)는 비 인가된 네트워크 장치의 ARP 테이블에서 게이트웨이의 MAC 주소를 의미 없는 주소로 변조시킴으로써, 비 인가된 네트워크 장치가 자신이 속한 서브넷 외부의 네트워크 장치에 접근하는 것을 차단할 수도 있다. 즉, 제어부(133)는 게이트웨이(예를 들어, L3 스위치(12))의 MAC 주소를 의미 없는 MAC 주소로 변조하기 위한 ARP 응답 패킷을 전송하여, 비 인가된 네트워크 장치의 ARP 테이블에서 게이트웨이의 MAC 주소를 의미 없는 MAC 주소로 변조시킬 수 있다. 이에 따라, 비 인가된 네트워크 장치는, 자신이 속한 서브넷의 다른 네트워크 장치 뿐만 아니라, 게이트웨이를 통해 접근해야 하는 다른 서브넷의 네트워크 장치 와도 통신이 차단될 수 있다.
- [85] 제어부(133)는 전송학 패킷 포워딩 방식을 사용하여 비 인가된 네트워크 장치가 다른 네트워크 장치에 접근하는 것을 차단할 수도 있다. 제어부(133)는 비 인가된 네트워크 장치가 검출되면, 비 인가된 네트워크 장치의 ARP 테이블에서 게이트웨이의 MAC 주소를 관리 장치(13)의 MAC 주소로 변조시키기 위한 ARP 응답 패킷을 비 인가된 네트워크 장치가 속한 서브넷으로 전송할 수 있다. 이에 따라, 비 인가된 네트워크 장치 내 ARP 테이블에서 게이트웨이의 MAC 주소는 관리 장치(13)의 MAC 주소로 변조되고, 비 인가된 네트워크 장치에 의해 전송된 패킷은 게이트웨이가 아닌 관리 장치(13)로 전달될 수 있다. 관리 장치(13)는 해당 네트워크 장치가 비 인가된 장치임을 이미 알고 있으므로, 비 인가된 네트워크 장치로부터 패킷이 수신되면, 이를 폐기하여 비 인가된 네트워크 장치의 통신을 차단할 수 있다.
- [86] 제어부(133)는 수신되는 패킷들을 분석하여, 네트워크 장치의 주소 도용(IP 주소 도용, MAC 주소 도용, IP 주소 및 MAC 주소 도용) 여부를 확인할 수도 있다.
- [87] 제어부(133)는 패킷이 수신되면, 수신된 패킷의 출발지 주소 정보를 정책 서버(43)에 등록된 장치들의 주소 정보와 비교하여 IP 주소 또는 MAC 주소를 도용한 네트워크 장치를 검출할 수 있다. 제어부(133)는 수집된 패킷에서 추출한 출발지 주소 정보가, 정책 서버(43)에 기 등록된 네트워크 장치와 IP 주소는 동일하나 MAC 주소가 상이하면, 해당 패킷을 전송한 네트워크 장치가 IP 주소를 도용한 것으로 결정할 수 있다. 또한, 제어부(133)는 수집된 패킷에서 추출한 출발지 주소 정보가, 정책 서버(43)에 기 등록된 네트워크 장치와 MAC 주소는 동일하나 IP 주소가 상이하면, 해당 패킷을 전송한 네트워크 장치가 MAC 주소를 도용한 것으로 결정할 수도 있다.
- [88] 제어부(133)는 각 네트워크 장치로부터 전송된 ARP 프로브(prob) 패킷을

분석하여, IP 및 MAC 주소를 도용한 네트워크 장치를 검출할 수도 있다.

- [89] IPv4 주소 충돌 감지 표준(IPv4 Address Conflict Detection, proposed standard)인 RFC 5227에서는, ARP 프로브 패킷에 대해 명시되어 있다. ACD에서 ARP 프로브 패킷은 호스트가 자신이 속해 있는 네트워크 내에서 자신의 IP 주소가 이미 사용 중인지 조사할 때 사용되는 패킷으로, IP 충돌을 방지하는 것을 목적으로 사용된다. 호스트는 ARP Opcode를 1로 설정하여 ARP 요청으로 설정된 ARP 프로브 패킷을 자신이 속한 네트워크 내에서 브로드캐스팅하고, 이에 대한 응답 패킷(ARP Opcode가 2인 패킷)의 수신을 대기한다. 호스트는 ARP 프로브 패킷(ARP 요청)의 전송 시, 헤더(header)의 출발지 MAC 주소를 자신의 MAC 주소로 설정하고, 출발지 IP 주소는 0.0.0.0으로 설정할 수 있다. 또한, 호스트는 ARP 프로브 패킷 헤더의 목적지 MAC 주소를 00:00:00:00:00:00으로 설정하고, 목적지 IP 주소는 자신의 IP 주소로 설정할 수 있다. 이러한 ARP 프로브 패킷은 IP 주소 충돌을 방지하기 위해 동일한 네트워크에 속하는 다른 호스트들의 ARP 테이블을 업데이트 시키지는 않는다.
- [90] 네트워크(1)에서 각 네트워크 장치(호스트)는 IP 주소가 변경되면, ARP 프로브 패킷을 반복해서 브로드캐스팅 하도록 작동한다. 따라서, 다른 네트워크 장치의 주소 데이터를 복제하여 자신의 IP 주소 및 MAC 주소를 변경한 도용 장치는, 복제된 IP 주소가 속한 네트워크 내에서 ARP 프로브 패킷을 브로드캐스팅하게 된다. 위에서 설명한 바와 같이, 각 네트워크 장치(호스트)로부터 전송된 ARP 프로브 패킷(ARP 요청)은 이를 전송한 네트워크 장치의 IP 주소 및 MAC 주소를 포함할 수 있다. 따라서, 제어부(133)는 네트워크 장치로부터 ARP 요청으로 전송된 ARP 프로브 패킷이 수신되면, 수신된 ARP 프로브 패킷으로부터 대응하는 네트워크 장치의 IP 주소 및 MAC 주소를 검출할 수 있다. 또한, 제어부(133)는 검출된 IP 주소 및 MAC 주소를 정책 서버(43)에 등록된 주소 정보와 비교하여, 해당 장치가 다른 네트워크 장치의 IP 주소 및 MAC 주소를 복제하여 사용하는 도용 장치인지를 판단할 수 있다.
- [91] 각 네트워크 장치는 IP 주소가 변경되는 때 외에도, 네트워크 인터페이스가 비활성 상태에서 활성 상태로 전환할 때, 네트워크 장치가 절전 모드에서 노멀(normal) 모드로 복귀할 때, 네트워크(1)와의 링크 상태(예를 들어, 이더넷 케이블의 연결 상태)에 변경이 발생했을 때, 802.11 무선 인터페이스가 새로운 기반 스테이션에 관련된 경우 등의 상황에서 ARP 프로브 패킷을 전송할 수도 있다. 즉, 도용 장치가 아닌 정상적인 네트워크 장치도 네트워크에 대한 연결이 오프라인 상태에서 온라인 상태로 전환되면, ARP 프로브 패킷을 반복해서 브로드캐스팅 할 수 있다.
- [92] 따라서, 제어부(133)는 정상적인 네트워크 장치를 도용 장치로 오 인식하는 것을 방지하기 위해, ARP 프로브 패킷을 전송한 네트워크 장치의 상태 정보를 추가로 확인할 수 있다. 제어부(133)는 ARP 프로브 패킷을 통해 새로 수집된 주소 정보와 동일한 주소 정보가 정책 서버(43)에 이미 등록된 상태이면,

대응하는 네트워크 장치의 ARP 프로브 패킷을 수신하기 전 상태 정보를 추가로 확인하여 주소 도용 여부를 최종 결정할 수도 있다. 즉, 제어부(133)는 ARP 프로브 패킷을 수신하기 전 대응하는 네트워크 장치의 상태 정보가 오프라인 상태를 지시하면, 수신된 ARP 프로브 패킷은 네트워크(1)와의 연결 상태가 온라인 상태로 전환된 정상적인 장치로부터 수신된 것으로 판단하여, 대응하는 네트워크 장치를 도용 장치가 아닌 정상적인 네트워크 장치로 최종 판단할 수 있다.

- [93] 제어부(133)는 전술한 바와 같이 다른 네트워크 장치의 주소 정보를 도용한 장치가 확인되면, 주소 도용 이벤트 발생을 정책 서버(43)에 통지할 수 있다. 또한, 정책 서버(43)로부터 수신한 정책 정보에 기초해, 검출된 도용 장치의 네트워크(1)에 대한 접근을 차단할 수 있다. 예를 들어, 제어부(133)는 도용 장치가 검출되면, 네트워크 사용 차단 패킷(ARP 프로브 패킷의 응답 패킷(ARP Probe Reply 패킷))을 전송하여 도용 장치의 네트워크 사용을 차단할 수 있다.
- [94] CCTV(31), 주차관리 시스템(32)과 같은 공용 시스템의 경우, 통상적으로 365일 24시간 온라인 상태를 유지하며, 맥내 단말(22) 및 아파트 단지 내 서버와의 통신이 항상 허용된다. 따라서, 누군가 악의적인 목적으로 이러한 공용 시스템의 주소를 도용할 경우 다른 네트워크 장치에 불법적인 접근이 가능할 수 있다. 네트워크(1)에서는 관리 장치(13)가 이러한 불법적인 주소 도용을 탐지하여 도용 장치가 다른 네트워크 장치에 접근하는 것을 사전에 차단함으로써, 공용 시스템의 주소를 도용하여 네트워크(1)에 침입하려는 시도를 차단할 수 있다.
- [95] 이하, 도 3 및 도 4를 참조하여 아파트 단지 내 네트워크(1)에서의 접근 통제 방법에 대해 설명한다.
- [96] 도 3은 일 실시 예에 따른 네트워크(1)에서 네트워크 장치들 간의 접근을 통제하는 방법을 개략적으로 도시한다. 도 3의 방법은 도 2를 참조하여 설명한 접근 통제 시스템(100)에 의해 수행될 수 있다.
- [97] 도 3을 참조하면, 관리 장치(13)는 작동이 개시되면 네트워크(1)에 등록된 각 네트워크 장치의 상태 정보 및 주소 정보를 획득할 수 있다(S11).
- [98] S11 단계에서, 관리 장치(13)는 ARP 요청 패킷을 전송하여 각 네트워크 장치의 상태 정보 및 주소 정보를 획득할 수 있다. 관리 장치(13)는 각 네트워크 장치에 대해 해당 네트워크 장치의 IP 주소를 목적지 주소 정보로 포함하는 ARP 요청 패킷을 생성하고, 이를 해당 네트워크 장치가 속한 서브넷으로 전송할 수 있다. 그런 다음, 제어부(133)는 전송된 ARP 요청 패킷에 대한 ARP 응답 패킷이 수신되는지 여부에 기초하여 대응하는 네트워크 장치의 상태 정보를 결정할 수 있다. 또한, 관리 장치(13)는 ARP 요청 패킷을 네트워크 장치들에 전송한 후 이에 대한 ARP 응답 패킷이 수신되면, 수신된 ARP 응답 패킷의 출발지 주소 정보로부터 각 네트워크 장치의 주소 정보(IP 주소 및 MAC 주소)를 획득할 수도 있다.
- [99] 관리 장치(13)는 각 네트워크 장치의 상태 정보 및 주소 정보가 확인되면, ARP

패킷을 사용해 각 네트워크 장치의 ARP 테이블에서 접근 통제가 필요한 네트워크 장치 및 게이트웨이의 MAC 주소를 변조시킬 수 있다(S12).

- [100] S12 단계에서, 관리 장치(13)는 맥내 단말(22)들 간의 통신을 차단하기 위해, 각 맥내 단말(22)의 ARP 테이블에서 다른 맥내 단말(22)의 MAC 주소를 의미 없는 주소로 변조시킬 수 있다. 이를 위해, 관리 장치(13)는 ARP 테이블 내 각 맥내 단말(22)의 MAC 주소를 변조하기 위한 변조된 ARP 응답 패킷을 생성할 수 있다. 각각의 변조된 ARP 응답 패킷은, 대응하는 맥내 단말(22)의 IP 주소와 변조된 MAC 주소(통신에 부적합한 MAC 주소)를 출발지 주소 정보로 포함할 수 있다. 관리 장치(13)는 이렇게 생성된 ARP 응답 패킷을 대응하는 맥내 단말(22)이 속한 서브넷(20)으로 전송할 수 있다. 이에 따라, 해당 서브넷(20)에 속한 맥내 단말(22)들의 ARP 테이블에서 대응하는 MAC 주소가 통신이 불가능한 MAC 주소로 변조되어, 대응하는 맥내 단말(22)에 대한 다른 맥내 단말의 접근이 차단될 수 있다. 관리 장치(13)는 이러한 방식으로, 각 맥내 단말(22)의 ARP 테이블에서 다른 맥내 단말들의 MAC 주소를 통신이 불가능한 주소로 모두 변경함으로써, 맥내 단말(22)들 간의 직접 통신을 모두 차단할 수 있다.
- [101] S12 단계에서, 관리 장치(13)는 서로 다른 서브넷(20, 30, 40) 간의 접근을 제한하기 위해, 각 네트워크 장치(22)의 ARP 테이블에서 게이트웨이의 MAC 주소를 관리 장치(13)의 MAC 주소로 변조시킬 수 있다. 이를 위해, 관리 장치(13)는 실제 게이트웨이의 IP 주소(L3 스위치(12)의 IP 주소)와 관리 장치(13)의 MAC 주소를 출발지 주소 정보로 포함하는 변조된 ARP 응답 패킷을 각 네트워크 장치가 속한 서브넷으로 전송할 수 있다. 이에 따라, 각 네트워크 장치의 ARP 테이블에서 게이트웨이의 MAC 주소가 관리 장치(13)의 MAC 주소로 변조될 수 있다. 따라서, 각 네트워크 장치는 자신이 속한 서브넷 외부로 패킷을 전달하고자 하는 경우 게이트웨이가 아닌 관리 장치(13)의 MAC 주소를 참조하여 패킷을 전송하고, 전송된 패킷은 게이트웨이 대신 관리 장치(13)에 수신될 수 있다.
- [102] ARP 테이블에서 게이트웨이의 MAC 주소를 변조한 후, 관리 장치(13)는 각 서브넷에 속한 네트워크 장치가 다른 네트워크(예를 들어, 다른 서브넷)로 전송한 패킷들을 게이트웨이 대신 수신할 수 있다(S13).
- [103] 관리 장치(13)는 패킷이 수신되면, 해당 패킷을 분석하여 패킷을 전송한 네트워크 장치, 즉 패킷의 출발지가 신규 네트워크 장치인지를 확인할 수 있다(S14).
- [104] S14 단계에서, 관리 장치(13)는 수신된 패킷으로부터 출발지 주소 정보(출발지 IP 주소 및 출발지 MAC 주소)를 획득하고, 이를 정책 서버(43)에 기 등록된 네트워크 장치들의 주소 정보와 비교할 수 있다. 관리 장치(13)는 기 등록된 네트워크 장치들의 주소 정보 중에서, 수신된 패킷으로부터 획득한 출발지 주소 정보와 동일한 주소 정보가 검색되지 않으면, 해당 패킷의 출발지가 네트워크(1)에 새로 연결된 신규 장치인 것으로 판단할 수 있다. 관리 장치(13)는

관리 장치(13)는 기 등록된 네트워크 장치들의 주소 정보 중에서, 수신된 패킷으로부터 획득한 출발지 주소 정보와 동일한 주소 정보가 검색되면, 해당 패킷의 출발지가 네트워크(1)에 이미 등록된 네트워크 장치인 것으로 판단할 수 있다.

- [105] 관리 장치(13)는 S14 단계를 통해 패킷 출발지가 네트워크(1)에 이미 등록된 네트워크 장치인 것으로 확인되면, 정책 서버(43)로부터 수신한 액세스 관리 정책에 기초해 수신된 패킷의 차단 여부를 결정할 수 있다(S15).
- [106] S15 단계에서, 관리 장치(13)는 수신된 패킷으로부터 출발지 IP 주소 및 목적지 IP 주소를 추출하고, VLAN 대역(또는 서브넷 대역) 간의 통신 허용 정책에서 출발지 IP 주소가 속한 서브넷과 목적지 IP 주소가 속한 서브넷 간의 통신을 허용하도록 설정되어 있는지 확인할 수 있다. 관리 장치(13)는 통신 허용 정책에서 출발지 IP 주소가 속한 VLAN 대역(서브넷 대역)과 목적지 IP 주소가 속한 VLAN 대역(서브넷 대역) 사이의 통신을 금지한 경우(예를 들어, 맥내 단말(22)이 다른 동(다른 서브넷(20))에 속한 맥내 단말(22)에 접속을 시도하는 경우), 해당 패킷의 차단이 필요한 것으로 판단할 수 있다. 반면에, 관리 장치(13)는 통신 허용 정책에서 출발지 IP 주소가 속한 VLAN 대역(서브넷 대역)과 목적지 IP 주소가 속한 VLAN 대역(서브넷 대역) 사이의 통신을 허용하는 경우(예를 들어, 맥내 단말(22)이 아파트 단지 내 공통으로 사용되는 네트워크 장치(예를 들어, CCTV(31), 주차관리 시스템(32), 단지 출입문(33), 공동 현관문(34) 등)에 접속을 시도하는 경우), 패킷을 차단할 필요가 없는 것으로 판단할 수 있다.
- [107] 관리 장치(13)는 정책에 의해 패킷의 차단이 필요하다면(S16), 해당 패킷을 폐기하여 통신을 차단할 수 있다(S17). 반면에, 관리 장치(13)는 패킷의 차단이 필요하지 않은 경우(S16), 해당 패킷을 실제 게이트웨이(예를 들어, L3 스위치(12))로 포워딩 하여(S18), 해당 패킷이 목적지에 정상적으로 전달되도록 할 수 있다.
- [108] 관리 장치(13)는 S14 단계에서 수신된 패킷의 출발지가 신규 네트워크 장치인 것으로 판단되면, 신규 네트워크 장치의 주소 정보를 정책 서버(43)에 전달하여 검출된 신규 네트워크 장치의 검출을 통보할 수 있다. 관리 장치(13)로부터 신규 네트워크 장치의 검출을 통보받은 정책 서버(43)는 정책 또는 관리자로부터 입력된 제어 입력에 기초해 신규 네트워크 장치의 인가 여부를 결정할 수 있다(S19). 정책 서버(43)는 신규 네트워크 장치가 인가된 장치이면(S20), 신규 네트워크 장치를 네트워크(1)에 등록하고(S21), 신규 네트워크 장치의 주소 정보를 데이터베이스(431)의 장치 정보에 포함시킬 수 있다.
- [109] 정책 서버(43)는 신규 네트워크 장치의 인가 여부가 결정되면, 인가 여부에 대한 정보를 관리 장치(13)에 전달할 수 있다. 이를 수신한 관리 장치(13)는 신규 네트워크 장치가 비 인가된 장치이면(S20), 비 인가된 장치의 네트워크(1)에 대한 접근을 차단할 수 있다(S22).

- [110] S22 단계에서, 관리 장치(13)는 변조된 ARP 응답 패킷을 사용하여 비 인가된 네트워크 장치의 ARP 테이블에서 비 인가된 네트워크 장치와 동일한 서브넷에 속하는 네트워크 장치들의 MAC 주소를 통신이 불가능한 의미 없는 MAC 주소로 변조할 수 있다. 이에 따라, 비 인가된 네트워크 장치는 자신과 동일한 서브넷에 속하는 다른 네트워크 장치의 올바른 MAC 주소를 확인할 수 없어 다른 네트워크 장치와의 통신이 차단된다.
- [111] S22 단계에서, 관리 장치(13)는 변조된 ARP 응답 패킷을 사용하여 비 인가된 네트워크 장치의 ARP 테이블에서 게이트웨이의 MAC 주소를 의미 없는 주소로 변조시킬 수도 있다. 이에 따라, 비 인가된 네트워크 장치는, 자신이 속한 서브넷의 다른 네트워크 장치 뿐만 아니라, 게이트웨이를 통해 접근해야 하는 다른 서브넷의 네트워크 장치와도 통신이 차단될 수 있다.
- [112] S22 단계에서, 관리 장치(13)는 ARP 패킷 변조 및 패킷 포워딩 방식을 사용하여 비 인가된 네트워크 장치가 다른 네트워크 장치에 접근하는 것을 차단할 수도 있다. 관리 장치(13)는 비 인가된 네트워크 장치가 검출되면, 비 인가된 네트워크 장치의 ARP 테이블에서 게이트웨이의 MAC 주소를 관리 장치(13)의 MAC 주소로 변조시키기 위한 ARP 응답 패킷을 비 인가된 네트워크 장치가 속한 서브넷으로 전송할 수 있다. 이에 따라, 비 인가된 네트워크 장치에 의해 전송된 패킷은 게이트웨이가 아닌 관리 장치(13)로 전달되고, 관리 장치(13)는 해당 네트워크 장치가 비 인가된 장치임을 이미 알고 있으므로, 비 인가된 네트워크 장치로부터 수신된 패킷을 폐기할 수 있다.
- [113] 도 4는 일 실시 예에 따른 네트워크(1)에서 주소 도용 장치의 접근을 차단하는 방법을 개략적으로 도시한다. 도 4의 방법은 도 2를 참조하여 설명한 접근 통제 시스템(100)에 의해 수행될 수 있다.
- [114] 도 4를 참조하면, 관리 장치(13)는 네트워크 장치들로부터 패킷들이 수집되면(S31), 각 패킷을 분석하여 패킷을 전송한 네트워크 장치들의 주소 도용 여부를 판단할 수 있다(S32).
- [115] S32 단계에서, 관리 장치(13)는 수집된 패킷의 출발지 주소 정보를 정책 서버(43)에 등록된 장치들의 주소 정보와 비교하여 IP 주소 또는 MAC 주소를 도용한 네트워크 장치를 검출할 수 있다. 관리 장치(13)는 수집된 패킷에서 추출한 출발지 주소 정보가, 정책 서버(43)에 기 등록된 네트워크 장치와 IP 주소는 동일하나 MAC 주소가 상이하면, 해당 패킷을 전송한 네트워크 장치가 IP 주소를 도용한 것으로 결정할 수 있다. 또한, 관리 장치(13)는 수집된 패킷에서 추출한 출발지 주소 정보가, 정책 서버(43)에 기 등록된 네트워크 장치와 MAC 주소는 동일하나 IP 주소가 상이하면, 해당 패킷을 전송한 네트워크 장치가 MAC 주소를 도용한 것으로 결정할 수도 있다.
- [116] S32 단계에서, 관리 장치(13)는 각 네트워크 장치로부터 전송된 ARP 프로브 패킷을 분석하여, IP 및 MAC 주소를 도용한 네트워크 장치를 검출할 수도 있다. 관리 장치(13)는 네트워크 장치로부터 ARP 요청으로 전송된 ARP 프로브

패킷으로부터 대응하는 네트워크 장치의 IP 주소 및 MAC 주소를 검출할 수 있다. 그런 다음, 관리 장치(13)는 검출된 IP 주소 및 MAC 주소를 정책 서버(43)에 등록된 주소 정보와 비교하여, 해당 장치가 다른 네트워크 장치의 IP 주소 및 MAC 주소를 복제하여 사용하는 도용 장치인지를 판단할 수 있다. 이 때, 관리 장치(13)는 정상적인 네트워크 장치를 도용 장치로 오 인식하는 것을 방지하기 위해, ARP 프로브 패킷을 전송한 네트워크 장치의 상태 정보를 추가로 확인할 수도 있다. 관리 장치(13)는 ARP 프로브 패킷을 수신하기 전 대응하는 네트워크 장치의 상태 정보가 오프라인 상태를 지시하면, 수신된 ARP 프로브 패킷은 네트워크(1)와의 연결 상태가 온라인 상태로 전환된 정상적인 장치로부터 수신된 것으로 판단하여, 대응하는 네트워크 장치를 도용 장치가 아닌 정상적인 네트워크 장치로 최종 판단할 수 있다.

- [117] 관리 장치(13)는 S32 단계를 통해 네트워크 장치가 주소 도용 장치로 확인되면(S33), 주소 도용 장치가 검출되었음을 정책 서버(43)에 통보할 수 있다(S34). 또한, 정책 서버(43)로부터 수신한 정책 정보에 기초해, 검출된 주소 도용 장치의 네트워크(1)에 대한 접근을 차단할 수 있다(S35). 예를 들어, 제어부(133)는 주소 도용 장치가 검출되면, 네트워크 사용 차단 패킷(ARP 프로브 패킷의 응답 패킷)을 전송하여 도용 장치의 네트워크 사용을 차단할 수 있다.
- [118] 관리 장치(13)는 S32 단계를 통해 네트워크 장치가 주소 도용 장치가 아닌 것 확인되면(S33), 설정된 정책에 따라서 네트워크 장치로부터 수신한 패킷들을 처리할 수 있다(S36). 예를 들어, 도 3의 S14 단계 내지 S22 단계를 통해 패킷들을 처리할 수 있다.
- [119] 전술한 실시 예에 따르면, 접근 통제 시스템(100)은 변조된 ARP 패킷을 사용해 각 맥내 단말(22)이 보유하는 다른 맥내 단말(22)의 MAC 주소를 통신이 불가능한 주소로 변조함으로써, 같은 서브넷(20)에 등록된 맥내 단말(22)들 간에 직접 통신을 효과적으로 차단할 수 있다.
- [120] 또한, 접근 통제 시스템(100)은 각 네트워크 장치가 보유한 게이트웨이의 MAC 주소를 관리 장치(13)의 MAC 주소로 변조하여, 관리 장치(13)가 게이트웨이 대신 패킷들을 수신한 뒤 정책에 따라 패킷들을 폐기하거나 포워딩 하도록 함으로써, 서로 통신이 허용되지 않은 서브넷들(예를 들어, 서로 다른 동의 맥내 단말(22)들이 연결된 서브넷(20)들) 간의 접근 또한 효과적으로 차단할 수 있다.
- [121] 또한, 접근 통제 시스템(100)의 관리 장치(13)에서 수집된 패킷들을 분석하여 비 인가된 네트워크 장치 또는 주소 도용 장치의 접근을 검출하여 사전에 차단할 수도 있다.
- [122] 전술한 실시 예들은, 프로그램이 기록된 매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 매체는, 컴퓨터 시스템에 의하여 읽힐 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 매체의 예로는, HDD(Hard Disk Drive), SSD(Solid State Disk), SDD(Silicon Disk Drive), ROM, RAM, CD-ROM, 자기

테이프, 플로피 디스크, 광 데이터 저장 장치 등이 있으며, 또한 캐리어 웨이브(예를 들어, 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한, 컴퓨터는 단말기의 제어부를 포함할 수도 있다. 따라서, 상기의 상세한 설명은 모든 면에서 제한적으로 해석되어서는 아니되고 예시적인 것으로 고려되어야 한다. 본 발명의 범위는 첨부된 청구항의 합리적 해석에 의해 결정되어야 하고, 본 발명의 등가적 범위 내에서의 모든 변경은 본 발명의 범위에 포함된다.

청구범위

- [청구항 1] 서로 다른 세대에 위치하는 복수의 맥내 단말을 포함하는 네트워크에서의 접근 통제 방법으로서,
관리 장치가, ARP(Address Resolution Protocol) 요청 패킷들을 상기 복수의 맥내 단말에 전송하는 단계,
상기 관리 장치가, 상기 ARP 요청 패킷에 대응하여 수신되는 제1 ARP 응답 패킷들을 분석하여 상기 복수의 맥내 단말의 주소 정보를 획득하는 단계,
상기 관리 장치가, MAC(Media Access Control) 주소가 변조된 제2 ARP 응답 패킷들을 생성하는 단계, 그리고
상기 관리 장치가, 상기 제2 ARP 응답 패킷들을 상기 복수의 맥내 단말에 전송함으로써, 상기 복수의 맥내 단말의 ARP 테이블에서 각 맥내 단말의 MAC 주소를 변조시키는 단계를 포함하며,
상기 제2 ARP 응답 패킷은, 각 ARP 테이블에서 MAC 주소를 변조하고자 하는 맥내 단말의 IP 주소와 변조된 MAC 주소를 출발지 주소 정보로 포함하는 ARP 응답 패킷이며,
상기 변조된 MAC 주소는 통신이 불가능한 MAC 주소인, 접근 통제 방법.
- [청구항 2] 제1항에 있어서,
상기 네트워크는, 서로 다른 네트워크 장치가 연결된 복수의 서브넷 각각에 대한 VLAN(Virtual Local Area Network) 대역 할당 정책 및 통신 허용 정책을 포함하는 액세스 관리 정책을 관리하는 정책 서버와, 상기 복수의 맥내 단말을 포함하는 복수의 네트워크 장치를 포함하며,
상기 접근 통제 방법은,
상기 관리 장치가, 상기 복수의 네트워크 장치에 MAC 주소가 변조된 제3 ARP 응답 패킷을 전송하여, 상기 복수의 네트워크 장치의 ARP 테이블에서 게이트웨이의 MAC 주소를 상기 관리 장치의 MAC 주소로 변조시키는 단계,
상기 관리 장치가, 상기 복수의 네트워크 장치로부터 게이트웨이로 전송된 패킷을 수신하는 단계, 그리고,
상기 관리 장치가, 상기 액세스 관리 정책에 기초해 수신된 패킷을 상기 게이트웨이로 전달하거나 폐기하는 단계를 더 포함하는 접근 통제 방법.
- [청구항 3] 제2항에 있어서,
상기 수신된 패킷을 상기 게이트웨이로 전달하거나 폐기하는 단계는,
상기 통신 허용 정책에서 상기 수신된 패킷의 목적지 IP 주소가 속한 VLAN 대역과 상기 수신된 패킷의 출발지 IP 주소가 속한 VLAN 대역 간의 통신이 금지된 경우, 상기 수신된 패킷을 폐기하는 단계를 포함하는, 접근 통제 방법.

- [청구항 4] 제2항에 있어서,
상기 수신된 패킷을 상기 게이트웨이로 전달하거나 폐기하는 단계는,
상기 통신 허용 정책에서 상기 수신된 패킷의 목적지 IP 주소가 속한
VLAN 대역과 상기 수신된 패킷의 출발지 IP 주소가 속한 VLAN 대역
간의 통신을 허용하는 경우, 상기 수신된 패킷을 상기 게이트웨이로
전달하는 단계를 포함하는, 접근 통제 방법.
- [청구항 5] 제2항에 있어서,
상기 수신된 패킷을 상기 게이트웨이로 전달하거나 폐기하는 단계는,
상기 수신된 패킷의 목적지 IP 주소가 상기 네트워크의 외부 네트워크에
속하면, 상기 수신된 패킷을 상기 게이트웨이에 전달하는 단계를
포함하는, 접근 통제 방법.
- [청구항 6] 제2항에 있어서,
상기 통신 허용 정책은, 상기 복수의 맥내 단말이 속한 서브넷들 간에는
통신이 금지되도록 설정되는, 접근 통제 방법.
- [청구항 7] 제2항에 있어서,
상기 관리 장치가, 상기 수신된 패킷으로부터 패킷을 전송한 네트워크
장치의 주소 정보를 획득하는 단계, 그리고
상기 관리 장치가, 상기 수신된 패킷으로부터 획득한 주소 정보와 상기
정책 서버에서 관리하는 주소 정보를 비교하여 신규 네트워크 장치를
검출하는 단계를 더 포함하는 접근 통제 방법.
- [청구항 8] 제7항에 있어서,
상기 액세스 관리 정책은, 상기 신규 네트워크 장치의 인가 여부를
결정하기 위한 정책을 더 포함하며,
상기 접근 통제 방법은,
상기 정책 서버가, 상기 액세스 관리 정책 또는 관리자로부터 입력되는
제어 입력에 기초해 상기 신규 네트워크 장치의 인가 여부를 결정하는
단계, 그리고
상기 관리 장치가, 상기 신규 네트워크 장치가 비 인가된 장치이면, 상기
신규 네트워크 장치의 ARP 테이블에서 다른 네트워크 장치의 MAC
주소를 통신이 불가능한 MAC 주소로 변조하기 위한 제4 ARP 요청
패킷을 상기 신규 네트워크 장치에 전송하는 단계를 더 포함하는 접근
통제 방법.
- [청구항 9] 제8항에 있어서,
상기 관리 장치가, 상기 신규 네트워크 장치가 비 인가된 장치이면, 상기
신규 네트워크 장치의 ARP 테이블에서 게이트웨이의 MAC 주소를
통신이 불가능한 MAC 주소 또는 상기 관리 장치의 MAC 주소로
변조하기 위한 제5 ARP 요청 패킷을 상기 신규 네트워크 장치에
전송하는 단계를 더 포함하는 접근 통제 방법.

- [청구항 10] 제2항에 있어서,
 상기 액세스 관리 정책은, 주소 도용 장치에 대한 차단 정책을 더 포함하며,
 상기 접근 통제 방법은,
 상기 관리 장치가, 상기 수신된 패킷으로부터 획득한 주소 정보와 상기 정책 서버에서 관리하는 주소 정보를 비교하여 상기 네트워크에 등록된 다른 네트워크 장치의 주소를 도용한 상기 주소 도용 장치를 검출하는 단계, 그리고
 상기 관리 장치가, 상기 차단 정책에 기초해 상기 주소 도용 장치를 상기 네트워크로부터 차단하는 단계를 더 포함하는 접근 통제 방법.
- [청구항 11] 제1항에 있어서,
 상기 관리 장치는, L3 스위치의 802.1Q 태그드 포트(802.1Q Tagged port)에 연결되는, 접근 통제 방법.
- [청구항 12] 서로 다른 세대에 위치하는 복수의 맥내 단말을 포함하는 네트워크에서의 접근 통제 시스템으로서,
 ARP(Address Resolution Protocol) 요청 패킷들을 상기 복수의 맥내 단말에 전송하고, 상기 ARP 요청 패킷에 대응하여 수신되는 제1 ARP 응답 패킷들을 분석하여 상기 복수의 맥내 단말의 주소 정보를 획득하며,
 MAC(Media Access Control) 주소가 변조된 제2 ARP 응답 패킷들을 상기 복수의 맥내 단말에 전송함으로써, 상기 복수의 맥내 단말의 ARP 테이블에 등록된 각 맥내 단말의 MAC 주소를 변조시켜 상기 복수의 맥내 단말 간의 통신을 차단하는 관리 장치를 포함하고,
 상기 제2 ARP 응답 패킷은, 각 ARP 테이블에서 MAC 주소를 변조하고자 하는 맥내 단말의 IP 주소와 변조된 MAC 주소를 출발지 주소 정보로 포함하는 ARP 응답 패킷이며,
 상기 변조된 MAC 주소는 통신이 불가능한 MAC 주소인, 접근 통제 시스템.
- [청구항 13] 제12항에 있어서,
 상기 네트워크를 구성하는 복수의 서브넷 각각에 대한 VLAN(Virtual Local Area Network) 대역 할당 정책 및 통신 허용 정책을 포함하는 액세스 관리 정책을 관리하는 정책 서버를 더 포함하고,
 상기 관리 장치는, 상기 네트워크에 등록된 복수의 네트워크 장치에 MAC 주소가 변조된 제3 ARP 응답 패킷을 전송하여 상기 복수의 네트워크 장치의 ARP 테이블에 등록된 게이트웨이의 MAC 주소를 상기 관리 장치의 MAC 주소로 변조시키고, 상기 복수의 네트워크 장치로부터 패킷이 수신되면 상기 액세스 관리 정책에 기초해 수신된 패킷을 상기 게이트웨이로 전달하거나 폐기하며,
 상기 복수의 네트워크 장치는, 상기 복수의 맥내 단말을 포함하는, 접근

- 통제 시스템.
- [청구항 14] 제13항에 있어서,
상기 관리 장치는, 상기 통신 허용 정책에서 상기 수신된 패킷의 목적지 IP 주소가 속한 VLAN 대역과 상기 수신된 패킷의 출발지 IP 주소가 속한 VLAN 대역 간의 통신이 금지된 경우, 상기 수신된 패킷을 폐기하는, 접근 통제 시스템.
- [청구항 15] 제13항에 있어서,
상기 관리 장치는, 상기 통신 허용 정책에서 상기 수신된 패킷의 목적지 IP 주소가 속한 VLAN 대역과 상기 수신된 패킷의 출발지 IP 주소가 속한 VLAN 대역 간의 통신을 허용하거나, 상기 수신된 패킷의 목적지 IP 주소가 상기 네트워크의 외부 네트워크에 속하면, 상기 수신된 패킷을 상기 게이트웨이에 전달하는, 접근 통제 시스템.
- [청구항 16] 제13항에 있어서,
상기 통신 허용 정책은, 상기 복수의 맥내 단말이 속한 서로 다른 서브넷 간에는 통신이 금지되도록 설정되는, 접근 통제 시스템.
- [청구항 17] 제13항에 있어서,
상기 정책 서버는, 상기 복수의 네트워크 장치의 주소 정보를 관리하며,
상기 관리 장치는, 상기 수신된 패킷으로부터 패킷을 전송한 네트워크 장치의 주소 정보를 획득하고, 상기 수신된 패킷으로부터 획득한 주소 정보와 상기 정책 서버에서 관리하는 주소 정보를 비교하여 신규 네트워크 장치를 검출하는, 접근 통제 시스템.
- [청구항 18] 제17항에 있어서,
상기 액세스 관리 정책은, 상기 신규 네트워크 장치의 인가 여부를 결정하기 위한 정책을 더 포함하며,
상기 정책 서버는, 상기 액세스 관리 정책 또는 관리자로부터 입력되는 제어 입력에 기초해 상기 신규 네트워크 장치의 인가 여부를 결정하고,
상기 관리 장치는, 상기 신규 네트워크 장치가 비 인가된 장치이면, 상기 신규 네트워크 장치의 ARP 테이블에서 다른 네트워크 장치의 MAC 주소를 통신이 불가능한 MAC 주소로 변조하기 위한 제4 ARP 요청 패킷을 상기 신규 네트워크 장치에 전송하는, 접근 통제 시스템.
- [청구항 19] 제18항에 있어서,
상기 관리 장치는, 상기 신규 네트워크 장치가 비 인가된 장치이면, 상기 신규 네트워크 장치의 ARP 테이블에서 게이트웨이의 MAC 주소를 통신이 불가능한 MAC 주소 또는 상기 관리 장치의 MAC 주소로 변조하기 위한 제5 ARP 요청 패킷을 상기 신규 네트워크 장치에 전송하는, 접근 통제 시스템.
- [청구항 20] 제13항에 있어서,
상기 액세스 관리 정책은, 주소 도용 장치에 대한 차단 정책을 더

포함하며,

상기 관리 장치는, 상기 수신된 패킷으로부터 획득한 주소 정보와 상기 정책 서버에서 관리하는 주소 정보를 비교하여 상기 네트워크에 등록된 다른 네트워크 장치의 주소를 도용한 상기 주소 도용 장치를 검출하며, 상기 차단 정책에 기초해 상기 주소 도용 장치를 상기 네트워크로부터 차단하는, 접근 통제 시스템.

[청구항 21]

제12항에 있어서,

상기 관리 장치는, L3 스위치의 802.1Q 태그드 포트(802.1Q Tagged port)에 연결되는, 접근 통제 시스템.