



(19) 대한민국특허청(KR)  
(12) 등록특허공보(B1)

(45) 공고일자 2011년05월17일  
(11) 등록번호 10-1034938  
(24) 등록일자 2011년05월06일

(51) Int. Cl.

H04W 8/26 (2009.01)

(21) 출원번호 10-2009-0115013  
(22) 출원일자 2009년11월26일  
심사청구일자 2009년11월26일

(56) 선행기술조사문헌  
KR1020090058881 A  
KR1020080036496 A  
KR1020070002100 A  
KR1020050016716 A

(73) 특허권자

삼성에스디에스 주식회사  
서울 강남구 역삼동 707-19

(72) 발명자

박선욱  
경기도 과천시 원문동 래미안슈르 아파트 340동 404호

안세준

경기도 과천시 별양동 뉴코아 7층 삼성네트웍스

정승훈

대구광역시 달서구 상인동 1145-1 상인아트빌 10 1동 401호

(74) 대리인

유수미

전체 청구항 수 : 총 15 항

심사관 : 정윤석

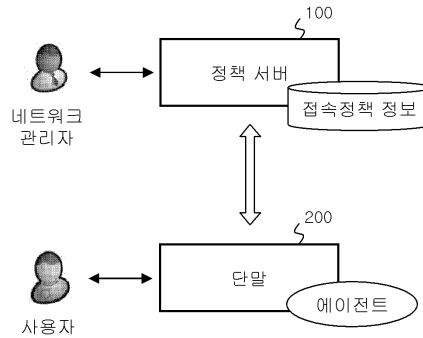
(54) IPv6 주소 및 접속정책 관리 시스템 및 방법

(57) 요약

본 발명은 IPv6 주소 및 접속정책 관리 시스템 및 방법에 관한 것이다.

본 발명에 따른 IPv6 주소 및 접속정책 관리 시스템 및 방법은, 정책 서버에서 사용자별 또는 사용자 그룹별로 IPv6 주소 및 네트워크 접속정책을 설정하여 사용자별 접속정책 정보를 생성하고, 사용자 단말이 상기 정책에 접속하여 사용자 인증을 수행한 후 사용자에게 해당하는 접속정책 정보를 수신하면, 상기 사용자 단말이 상기 접속정책 정보에 근거하여 단말의 IPv6 주소 및 접속정책 기능을 설정하는 것을 특징으로 한다.

대표도 - 도1



## 특허청구의 범위

### 청구항 1

IPv6 주소 및 접속정책 관리 시스템으로서,

사용자별 또는 사용자 그룹별로 설정된 네트워크 접속정책 정보를 관리하는 정책 서버; 및

상기 정책 서버에 접속하여 사용자 인증을 수행한 후 사용자에게 해당하는 접속정책 정보를 수신하고, 상기 접속정책 정보에 근거하여 단말의 IPv6 주소 및 접속정책 기능을 자동으로 설정하는 에이전트 모듈을 구비하는 사용자 단말을 포함하는 IPv6 주소 및 접속정책 관리 시스템.

### 청구항 2

제1항에 있어서,

상기 사용자 단말의 IPv6 주소는 사업장 서브넷(subnet) 주소에 상응하는 프리픽스(prefix) 64비트와 이전 할당된 IPv4 주소 및 사용자 접속정책에 상응하는 호스트(host) 64비트로 구성되는 것을 특징으로 하는 IPv6 주소 및 접속정책 관리 시스템.

### 청구항 3

제2항에 있어서,

상기 호스트 64비트는 사용자의 보안등급을 포함하는 것을 특징으로 하는 IPv6 주소 및 접속정책 관리 시스템.

### 청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 접속정책 정보는 단말 주소 설정 기능, 단말 주소 설정시 재부팅 옵션 추가 기능, 디폴트 게이트웨이 설정 기능, DNS(Domain Name Service) 서버 주소 설정 기능, 터널 기능 온(on) 또는 오프(off) 기능, 네이버 캐시(Neighbor cache) 삭제 기능, 주소 숨김(Privacy Extension) 온 또는 오프 기능 중 적어도 하나에 대한 정보를 포함하는 것을 특징으로 하는 IPv6 주소 및 접속정책 관리 시스템.

### 청구항 5

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 정책 서버 및 상기 사용자 단말은 IPv4 및 IPv6 듀얼 스택(dual stack)을 지원하며, 사용자 인증을 위해 상기 정책 서버와 상기 사용자 단말은 IPv4 및 IPv6 링크 로컬 주소(link local address)를 사용하는 것을 특징으로 하는 IPv6 주소 및 접속정책 관리 시스템.

### 청구항 6

IPv6 주소 및 접속정책 관리를 위한 정책 서버로서,

사용자별 또는 사용자 그룹별로 할당할 IPv6 주소 및 네트워크 접속정책을 설정하여 사용자별 접속정책 정보를 생성하는 접속정책 설정부;

사용자 단말이 접속하면, 상기 사용자 단말에게 사용자 정보를 요구하여 사용자에게 대한 인증을 수행하는 사용자 인증부; 및

상기 접속정책 설정부에서 생성된 사용자별 접속정책 정보를 저장하는 접속정책 저장부를 포함하는 것을 특징으로 하는 정책 서버.

### 청구항 7

제6항에 있어서,

상기 정책 서버는 상기 사용자 단말로부터 접속정책 정보가 요청되면, 상기 사용자 인증부에서 인증된 사용자에게 상응하는 접속정책 정보를 상기 사용자 단말로 전송하는 것을 특징으로 하는 정책 서버.

**청구항 8**

제6항 또는 제7항에 있어서,

상기 접속정책 정보는 단말 주소 설정 기능, 단말 주소 설정시 재부팅 옵션 추가 기능, 디폴트 게이트웨이 설정 기능, DNS(Domain Name Service) 서버 주소 설정 기능, 터널 기능 온(on) 또는 오프(off) 기능, 네이버 캐시(Neighbor cache) 삭제 기능, 주소 숨김(Privacy Extension) 온 또는 오프 기능 중 적어도 하나에 대한 정보를 포함하는 것을 특징으로 하는 정책 서버.

**청구항 9**

제6항 또는 제7항에 있어서,

상기 정책 서버는 IPv4 및 IPv6 듀얼 스택(dual stack)을 지원하며, 사용자 인증을 위해 상기 사용자 단말과의 통신 시 IPv4 및 IPv6 링크 로컬 주소(link local address)를 사용하는 것을 특징으로 하는 정책 서버.

**청구항 10**

제6항 또는 제7항에 있어서,

상기 IPv6 주소는 사업장 서브넷(subnet) 주소에 상응하는 프리픽스(prefix) 64비트와 이전 할당된 IPv4 주소, 사용자 접속정책, 및 보안등급을 포함하는 호스트(host) 64비트로 구성되는 것을 특징으로 하는 정책 서버.

**청구항 11**

제6항 또는 제7항에 있어서,

상기 사용자 단말이 접속하면, 상기 사용자 단말의 IP(Internet Protocol) 주소, MAC(Media Access Control) 주소, 사용자명, 접속 시간을 저장하는 접속로그 저장부를 더 포함하는 것을 특징으로 하는 정책 서버.

**청구항 12**

IPv6 주소 및 접속정책 관리 방법으로서,

- a) 정책 서버에서 사용자별 또는 사용자 그룹별로 IPv6 주소 및 네트워크 접속정책을 설정하여 사용자별 접속정책 정보를 생성하는 단계;
- b) 사용자 단말이 상기 정책 서버에 접속하여 사용자 인증을 수행한 후 사용자에게 해당하는 접속정책 정보를 수신하는 단계; 및
- c) 상기 사용자 단말이 상기 접속정책 정보에 근거하여 단말의 IPv6 주소 및 접속정책 기능을 설정하는 단계를 포함하는 IPv6 주소 및 접속정책 관리 방법.

**청구항 13**

제12항에 있어서,

상기 단계 b)에서, 상기 사용자 단말의 접속정책 정보 수신은 IPv4 주소를 이용하여 수행되는 것을 특징으로 하는 IPv6 주소 및 접속정책 관리 방법.

**청구항 14**

제12항 또는 제13항에 있어서,

상기 접속정책 정보는 단말 주소 설정 기능, 단말 주소 설정시 재부팅 옵션 추가 기능, 디폴트 게이트웨이 설정 기능, DNS(Domain Name Service) 서버 주소 설정 기능, 터널 기능 온(on) 또는 오프(off) 기능, 네이버 캐시(Neighbor cache) 삭제 기능, 주소 숨김(Privacy Extension) 온 또는 오프 기능 중 적어도 하나에 대한 정보를 포함하는 것을 특징으로 하는 IPv6 주소 및 접속정책 관리 방법.

**청구항 15**

제12항 또는 제13항에 있어서,

상기 단말의 IPv6 주소는 사업장 서브넷(subnet) 주소에 상응하는 프리픽스(prefix) 64비트와 이전 할당된 IPv4 주소, 사용자 접속정책, 및 보안등급을 포함하는 호스트(host) 64비트로 구성되는 것을 특징으로 하는 IPv6 주소 및 접속정책 관리 방법.

**명세서**

**발명의 상세한 설명**

**기술분야**

[0001] 본 발명은 IPv6(Internet Protocol version 6) 주소 및 접속정책 관리 시스템 및 방법에 관한 것으로, 더욱 상세하게는 사용자에게 할당될 IPv6 주소 및 네트워크 접속정책을 정책 서버와 단말 간 통신을 활용하여 네트워크 관리자가 원격으로 관리하는 시스템 및 방법에 관한 것이다.

**배경기술**

[0002] 기존의 IP(Internet Protocol) 시스템은 32비트(bit)의 주소 체계를 갖는 IPv4(Internet Protocol version 4) 기술을 기반으로 하였다. 그러나, 인터넷 사용의 증가 및 유비쿼터스(Ubiquitous) 기술의 발달에 따라 32비트의 길이로는 할당할 수 있는 주소가 고갈되는 문제가 발생하였으며, 이를 해결하고자 IETF(Internet Engineering Task Force)에서는 128비트의 주소 체계를 사용하는 IPv6를 표준화하였다.

[0003] 하지만, IPv6 주소는 128비트의 길이를 갖기 때문에 IPv4 주소에 비해 주소가 매우 길고 복잡한 특성을 가진다. 따라서, 단말(예컨대, PC) 사용자가 직접 수동(manual)으로 단말의 IPv6 주소를 설정(setting)하는 경우는 매우 드물며, DHCPv6(Dynamic Host Configuration Protocol for IPv6), RA(Router Advertisement) 등을 통해 자동으로 주소를 할당하는 방법이 보편화되어 있다. 즉, IPv6 주소의 경우 DHCPv6, RA와 같은 동적 자동 주소할당 방법이 현재 대부분의 네트워크 환경에서 사용되고 있으며, 이와 같은 방식은 프로토콜 간 통신에 의해 자동으로 설정된다.

[0004] 그러나, 전술한 방법은 IPv6 주소를 일괄적으로 할당하기에는 편리하지만 특정 사용자를 위한 고정 주소를 할당하거나 접속을 제한하는 등의 접속정책 관리는 거의 수행할 수 없어 개인별 제어가 실질적으로 불가능한 문제가 있으며, 꼭 필요한 경우에는 사용자가 직접 단말을 수동으로 설정하여 제어해야만 한다. 특히, 기업 내부와 같이 보안이 중요시 되는 네트워크에서는 방화벽 룰 셋팅 및 특정 사용자의 접속 제한 등의 필요성이 발생할 수 있는데, 이 경우에는 사용자별로 IPv6 주소를 고정해야 할 필요가 있다.

[0005] 그러나, 기존의 장비 간 통신에 의한 동적 자동 할당방식으로는 개인별 IPv6 주소를 제어할 수 없고, Windows 기반의 PC에서는 RFC(Request For Comments) 4941에 의해 소스 IP 주소의 변경이 발생하는 등 방화벽에서 개인별 보안 룰을 적용할 수 없다. 또한, Windows 기반의 PC에서는 개인의 IPv6 사용을 위해 6to4와 같은 자동 터널 생성 기능이 디폴트(Default)로 설정되어 있어 임의의 사용자 간 IPv6 통신이 인캡슐레이션(encapsulation)된 패킷을 통해 이루어지는 것을 보안 관리자가 알기 어려워, 기업 내부에서는 보안관리에 심각한 문제가 발생할 수 있다.

[0006] 그리고, 개인 단말에서 반드시 고정 IPv6 주소를 사용해야 하는 경우에는 사용자가 직접 수동으로 설정해야 하고, 주소 뿐 아니라 RFC 4941에 의한 임시주소 사용기능도 오프(off)시켜야 하므로 매우 불편한 문제가 있다. 또한, 네트워크 관리자 역시 내부 정책에 의한 IPv6 주소를 할당 관리할 수 없고, 비록 사용자가 수동으로 IPv6 주소를 설정했다 해도 정확하게 되었는지 네트워크 관리자가 원격에서는 알 수 없기 때문에 직접 확인해야 하는 불편함이 여전히 존재한다.

**발명의 내용**

**해결 하고자하는 과제**

[0007] 본 발명은 전술한 바와 문제점을 해결하기 위해 창안된 것으로, 본 발명의 목적은 사용자에게 할당될 IPv6 주소 및 네트워크 접속정책을 정책 서버와 단말 간 통신을 활용하여 네트워크 관리자가 원격으로 관리할 수 있는 시스템 및 방법을 제공하는 것이다.

[0008] 본 발명의 다른 목적은 IPv6 단말에 정책 서버와 통신이 가능한 에이전트(Agent)를 설치하고, 에이전트가 정책 서버로부터 IPv6 주소 할당, 접속 허용 사업장, 주소 숨김 기능 사용 등에 대한 접속정책 정보를 다운로드하여

IPv6 단말을 설정하게 함으로써, 네트워크 관리자가 IPv6 주소 및 접속정책을 원격으로 관리할 수 있는 시스템 및 방법을 제공하는 것이다.

[0009] 본 발명의 또 다른 목적은 단말의 IPv6 주소 설정시 기존 할당된 IPv4 주소, 사업장의 서브넷 주소, 구체적 접속정책, 보안등급 등의 정보가 포함되도록 함으로써, 보안 등과 같은 네트워크 관리를 용이하게 수행할 수 있는 시스템 및 방법을 제공하는 것이다.

**과제 해결수단**

[0010] 상기한 목적을 위하여, 본 발명의 일 형태에 따른 IPv6 주소 및 접속정책 관리 시스템은, 사용자별 또는 사용자 그룹별로 설정된 네트워크 접속정책 정보를 관리하는 정책 서버; 및 상기 정책 서버에 접속하여 사용자 인증을 수행한 후 사용자에게 해당하는 접속정책 정보를 수신하고, 상기 접속정책 정보에 근거하여 단말의 IPv6 주소 및 접속정책 기능을 자동으로 설정하는 에이전트 모듈을 구비하는 사용자 단말을 포함하는 것을 특징으로 한다.

[0011] 그리고, 본 발명의 일 형태에 따른 IPv6 주소 및 접속정책 관리를 위한 정책 서버는, 사용자별 또는 사용자 그룹별로 할당할 IPv6 주소 및 네트워크 접속정책을 설정하여 사용자별 접속정책 정보를 생성하는 접속정책 설정부; 사용자 단말이 접속하면, 상기 사용자 단말에게 사용자 정보를 요구하여 사용자에게 대한 인증을 수행하는 사용자 인증부; 및 상기 접속정책 설정부에서 생성된 사용자별 접속정책 정보를 저장하는 접속정책 저장부를 포함하는 것을 특징으로 한다.

[0012] 한편, 본 발명의 일 형태에 따른 IPv6 주소 및 접속정책 관리 방법은, a) 정책 서버에서 사용자별 또는 사용자 그룹별로 IPv6 주소 및 네트워크 접속정책을 설정하여 사용자별 접속정책 정보를 생성하는 단계; b) 사용자 단말이 상기 정책 서버에 접속하여 사용자 인증을 수행한 후 사용자에게 해당하는 접속정책 정보를 수신하는 단계; 및 c) 상기 사용자 단말이 상기 접속정책 정보에 근거하여 단말의 IPv6 주소 및 접속정책 기능을 설정하는 단계를 포함하는 것을 특징으로 한다.

**효과**

[0013] 본 발명에 따르면, 기존의 자동 주소할당 방식으로는 불가능했던 사용자별 IPv6 주소 할당과 함께 접속정책을 네트워크 관리자가 원격으로 제어 관리할 수 있는 효과를 가진다. 즉, Windows 등의 단말이 IPv6 터널을 자동 생성하여 외부의 사용자와 허가받지 않은 통신을 수행하거나 단말이 RFC4941에 의한 임시 주소를 사용함으로써 특정 사용자가 어느 사이트에 접속했는지 알 수 없는 문제점을 해결하여, 기업 내부의 보안 관리를 보다 강화할 수 있는 효과를 가진다.

[0014] 그리고, 본 발명에 따르면, 사용자별 IPv6 주소를 정책적으로 할당해야 할 경우, 사용자가 수동으로 IPv6 주소를 설정하던 종래 방식과는 단말에 설치된 에이전트 모듈을 통해 자동으로 수행함으로써, 사용자별 IPv6 주소를 용이하게 할당할 수 있는 효과를 가진다.

[0015] 또한, 본 발명에 따르면, 네트워크 관리자가 정책 서버를 통해 사용자별 접속정책을 제어함으로써, 사용자 단말을 효율적으로 일괄 관리할 수 있는 효과를 가진다.

[0016] 또한, 본 발명에 따르면, 정책 서버와 단말 간 기본통신을 IPv4로 사용할 수 있기 때문에, IPv6 만 사용하는 환경 뿐 아니라 IPv4와 IPv6가 혼재하는 환경에서도 효율적으로 동작이 가능한 효과를 가진다.

**발명의 실시를 위한 구체적인 내용**

[0017] 이하에서는 첨부 도면 및 바람직한 실시예를 참조하여 본 발명을 상세히 설명한다. 참고로, 하기 설명에서 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략한다.

[0018] 먼저, 도 1은 본 발명에 따른 IPv6 주소 및 접속정책 관리 시스템의 구성도이다.

[0019] 도 1을 참고하면, 본 발명에 따른 IPv6 주소 및 접속정책 관리 시스템은 네트워크 관리자에 의해 제어되는 정책 서버(100)와 개별 사용자가 네트워크 접속을 위해 사용하는 적어도 하나의 단말(200)로 구성된다. 여기서, 정책 서버(100)에는 네트워크 관리자에 의해 사용자별 또는 사용자 그룹별로 설정된 접속정책 정보가 저장되며, 단말(200)에는 에이전트(Agent) 모듈이 구비되어 정책 서버(100)로부터 접속정책 정보를 수신하여 IPv6 주소 및 접속정책 기능을 설정한다.

[0020] 이와 관련하여, 도 2는 본 발명에 따른 정책 서버(100)의 상세 구성도를 예시한 것이다. 도시된 바와 같이, 본

발명에 따른 정책 서버(100)는 접속정책 설정부(110), 사용자 인증부(120), 접속로그 저장부(130), 접속정책 저장부(140) 등을 포함한다.

- [0021] 접속정책 설정부(110)는 사용자별 또는 사용자 그룹별로 할당할 IPv6 주소 및 네트워크 접속정책을 설정하는 기능을 수행한다. 즉, 네트워크 관리자는 접속정책 설정부(110)를 통해 사용자별 또는 사용자 그룹별로 IPv6 주소 및 네트워크 접속정책을 설정(입력)함으로써, 사용자 단말(200)에 대한 IPv6 주소 및 접속정책을 원격으로 관리한다.
- [0022] 사용자별 또는 사용자 그룹별로 관리하는 네트워크 접속정책의 예로는, 도 3에 도시된 바와 같이, 단말 주소 설정(고정 IP 또는 유동 IP 할당) 기능, 단말 주소 설정시 재부팅 옵션 추가 기능, 디폴트 게이트웨이 설정 기능, DNS(Domain Name Service) 서버 주소 설정 기능, 터널 기능 온(on)/오프(off) 기능, 네이버 캐시(Neighbor cache) 삭제 기능, 주소 숨김(Privacy Extension) 온/오프 기능 등을 들 수 있으며, 접속정책 설정부(110)는 이와 같이 네트워크 관리자에 의해 설정된 구체적 접속정책을 사용자와 매칭시켜 접속정책 정보를 생성한다.
- [0023] 사용자 인증부(120)는 사용자 단말(200)이 정책 서버(100)로 사용자 접속정책 정보를 요청하면, 해당 단말(200)의 사용자 정보를 요구하여 사용자에게 대한 인증을 수행한다. 사용자 인증은 예컨대 사용자 ID, 패스워드, 사용자 인적 사항, 사용자 단말의 MAC(Media Access Control) 주소 등을 통해 수행될 수 있으며, 보다 높은 보안 수준이 요구되는 경우 지문 인식 등과 같은 생체 정보를 이용하여 수행될 수도 있다.
- [0024] 접속로그 저장부(130)는 사용자 단말(200)이 정책 서버(100)에 접속하면, 해당 단말(200)의 IP(Internet Protocol) 주소, MAC(Media Access Control) 주소, 사용자명, 접속 시간, 접속 장소 등과 같은 사용자 접속 기록을 로그(log) 형태로 저장한다.
- [0025] 접속정책 저장부(140)는 네트워크 관리자가 접속정책 설정부(110)를 통해 설정한 사용자별 접속정책 정보를 데이터베이스(Database) 형태로 저장한다.
- [0026] 이상에서 본 발명에 따른 IPv6 주소 및 접속정책 관리 시스템을 대략적으로 설명하였는데, 각 구성요소의 구체적인 동작, 기능 등에 대하여는 본 발명에 따른 IPv6 주소 및 접속정책 관리 방법과 함께 상세 설명하도록 한다.
- [0027] 도 4는 본 발명에 따른 IPv6 주소 및 접속정책 관리 방법의 흐름도이다.
- [0028] 도 4를 참조하면, 단계 S410에서, 네트워크 관리자는 정책 서버(100)의 접속정책 설정부(110)를 통해 i) 회사의 각 사업장별 서브넷(subnet) 주소 설정(즉, IPv6 주소 프리픽스(prefix) 설정), ii) 자사 직원 여부, 부서, 직급 등과 관련된 사용자별 보안등급 설정, iii) 사용자 단말의 IPv6 주소(고정 IP 또는 유동 IP), 디폴트 게이트웨이, DNS 서버 주소, 터널 기능 온/오프, 네이버 캐시(Neighbor cache) 삭제, 주소 숨김(Privacy Extension) 온/오프 등과 같은 네트워크 정책정보 설정 등을 수행한다.
- [0029] 그리고, 단계 S420에서, 사용자 단말(200)(구체적으로는, 에이전트 모듈)이 정책 서버(100)에 접속하여 사용자 접속정책 정보를 요청하면, 단계 S430에서, 정책 서버(100)의 사용자 인증부(120)는 사용자 단말(200)에게 사용자 정보를 요청하여 사용자 인증을 수행한다. 이 경우 정책 서버(100)와 사용자 단말(200) 간 통신은 IPv4 통해 이루어진다. 즉, 본 발명에 따른 정책 서버(100)와 사용자 단말(200)은 IPv4 및 IPv6 듀얼 스택(dual stack)을 지원하며, 필요에 따라 정책 서버(100)와 사용자 단말(200) 간 통신시 IPv4 또는 IPv6 링크 로컬 주소(link local address)를 사용할 수 있다.
- [0030] 그리고, 정책 서버(100)의 사용자 인증부(120)에서 사용자 인증이 완료되면, 단계 S440에서, 사용자 단말(200)(구체적으로는, 에이전트 모듈)은 정책 서버(100)에 사용자 접속정책 정보를 요청하고, 정책 서버(100)는 단계 S430에서 인증된 사용자에게 해당하는 접속정책 정보를 사용자 단말(200)로 전송한다.
- [0031] 그러면, 단계 S450에서, 사용자 단말(200)(구체적으로는, 에이전트 모듈)은 정책 서버(100)로부터 전송받은 접속정책 정보에 근거하여 단말의 IPv6 주소 및 접속정책 기능을 설정한다.
- [0032] 부연하면, 사용자 단말(200)(구체적으로는, 에이전트 모듈)은 IPv4/IPv6 듀얼 스택 환경인 경우에는 먼저 IPv4 주소를 할당받은 후, 정책 서버(100)에 접속하여 사용자 인증을 수행하고 사용자 접속정책 정보를 다운로드받으며, 다운로드받은 사용자 접속정책 정보에 근거하여 단말(200)의 IPv6 주소 및 접속정책 기능을 설정한다.
- [0033] 참고로, 도 5는 본 발명의 일 실시예에 따라 사용자 접속정책 정보에 근거하여 단말의 IPv6 주소를 설정하는 것을 예시하였는데, 구체적으로는 기존에 할당된 IPv4 주소(32비트)를 활용하여 IPv6 주소를 설정하는 것을 예시

한 것이다. 도 5를 참조하면, 예컨대 사업장 서버넷 주소(64비트)를 IPv6 주소의 프리픽스(Prefix)로 사용하고, 기존에 할당된 IPv4 주소(32비트)와 터널 기능 온/오프, 주소 숨김 기능 온/오프 등과 같은 구체적인 접속정책(16비트) 및 자사 직원 여부, 부서, 직급 등과 관련된 보안등급(16비트)을 IPv6 주소의 호스트(Host)로 사용함으로써, 128비트의 IPv6 주소를 설정할 수 있다.

[0034] 물론, 전술한 도 5는 예시적인 것이며, 단말(200)의 IPv6 주소는 기존에 할당된 IPv4 주소와 상관없이 생성될 수 있으며, IPv6 주소의 프리픽스 및/또는 호스트는 도 5와 다르게 구성될 수 있다.

[0035] 한편, 본 발명에 따르면, 이와 같이 사용자 단말(200)이 에이전트 모듈을 통해 정책 서버(100)로부터 사용자 접속정책 정보를 수신하고 이에 근거하여 단말의 IPv6 주소 및 접속정책 기능을 설정하도록 함으로써, 사용자 단말(200)은 복잡한 IPv6 주소를 자동으로 설정할 수 있으며, 네트워크 관리자는 정책 서버(100)와 사용자 단말(200) 간 통신을 이용하여 사용자별 IPv6 주소 및 네트워크 접속정책을 원격으로 관리할 수 있다.

[0036] 지금까지 본 발명을 바람직한 실시예를 참조하여 상세히 설명하였지만, 본 발명이 속하는 기술분야의 당업자는 본 발명의 기술적 사상이나 필수적 특징들을 변경하지 않고서 다른 구체적인 다양한 형태로 실시할 수 있는 것이므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적인 것이 아닌 것으로서 이해해야만 한다.

[0037] 그리고, 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 특정되는 것이며, 특허청구 범위의 의미 및 범위 그리고 그 등가개념으로부터 도출되는 모든 변경 또는 변형된 형태는 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

**도면의 간단한 설명**

[0038] 도 1은 본 발명에 따른 IPv6 주소 및 접속정책 관리 시스템의 구성도이다.

[0039] 도 2는 본 발명에 따른 IPv6 주소 및 접속정책 관리를 위한 정책 서버의 구성도이다.

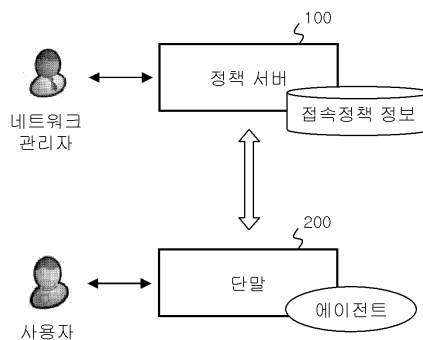
[0040] 도 3은 네트워크 관리자에 의해 설정되는 네트워크 접속정책을 예시하는 도면이다.

[0041] 도 4는 본 발명에 따른 IPv6 주소 및 접속정책 관리 방법의 흐름도이다.

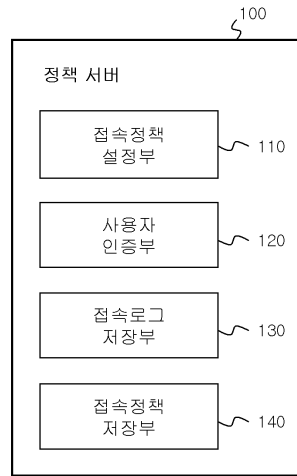
[0042] 도 5는 사용자 접속정책 정보에 근거하여 단말의 IPv6 주소를 설정하는 것을 예시하는 도면이다.

**도면**

**도면1**



도면2

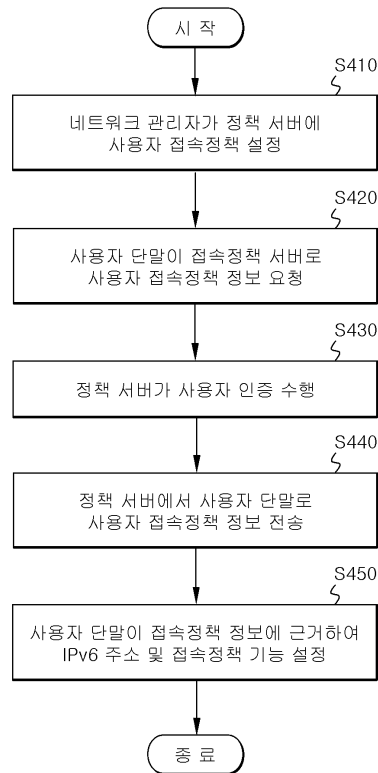


도면3

구분	기능	비고
접속정책	단말 주소 설정 기능	단말에 IPv6 주소 설정
	단말 주소 설정시 재부팅 옵션 추가 기능	단말 재부팅시 주소가 리셋되도록 설정
	디폴트 게이트웨이 설정 기능	단말의 IPv6 게이트 주소 설정
	DNS 서버 주소 설정 기능	IPv6 DNS 주소 설정
	터널 기능 on/off 기능	6to4, isatap, teredo 터널 기능 on/off 설정
	Neighbor cache 삭제 기능	Neighbor cache 삭제
	Privacy Extension on/off 기능	privacy extension 기능 on/off 설정



도면4



도면5

<IPv4 주소>

IPv4 주소 (32비트)
33:10:44:56

<IPv6 주소>

비트 구분	네트워크 Prefix (64비트)		Host (64비트)	
	사업장 subnet (64비트)	접속정책 (16비트)	보안등급 (16비트)	IPv4 주소 (32비트)
용도	2001:0330:A030:3010	0001	0001	33:10:44:56
할당 주소	2001:0330:A030:3010:0001:0001:210A:2C38			