(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[8]
H04L 12/24 (2006.01)

(45) 공고일자 2006년01월27일
(11) 등록번호 10-0524055
(24) 등록일자 2005년10월19일

(21) 출원번호 10-1998-0007318
(22) 출원일자 1998년03월05일

(65) 공개번호 10-1999-0074001
(43) 공개일자 1999년10월05일

(73) 특허권자 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 나승주
서울특별시 강남구 역삼동 631-13 다가구 101호

(74) 대리인 리엔목특허법인

심사관 : 신성길

(54) 원격지 웨이크 업 기능을 갖는 컴퓨터 시스템 및 컴퓨터 시스템의 원격 웨이크 업 방법

요약

본 발명은 비밀보장 원격지 웨이크 업 기능을 갖는 컴퓨터 시스템 및 그 컴퓨터 시스템의 원격 웨이크 업 방법에 관한 것으로서, 비밀보장 원격지 웨이크 업 기능을 갖는 컴퓨터 시스템은 네트워크 주소 및 패스워드를 포함한 네트워크 정보를 저장한 네트워크 정보 저장부; 및 매직 패킷을 수신하고 매직 패킷에 포함된 네트워크 주소 및 패스워드와 네트워크 정보 저장부에 저장된 네트워크 주소 및 패스워드를 비교하여, 네트워크 주소와 패스워드가 일치하는 경우에만 컴퓨터 시스템이 구비한 전원 관리 장치에 웨이크 업 제어신호를 전달하는 매직 패킷 제어기를 포함하고, 웨이크 업 제어신호에 의해 중지 상태에 있던 시스템을 다시 부팅함을 특징으로 한다.

본 발명에 의하면, 네트워크를 통해 다른 컴퓨터 시스템을 원격 웨이크 업할 때, 정당한 수퍼바이저에 의한 웨이크 업인지 여부를 확인함으로써 악의의 사용자로부터 컴퓨터 시스템의 정보가 유출되거나, 컴퓨터 시스템이 손상되는 것을 방지할 수 있다.

대표도

도 3

명세서

도면의 간단한 설명

도 1은 네트워크에 의해 접속된 컴퓨터 시스템들의 구성도이다.

도 2는 종래의 기술에 의한 컴퓨터 시스템의 원격 웨이크 업 과정을 도시한 흐름도이다.

도 3은 본 발명에 의한 컴퓨터 시스템의 네트워크 접속부의 구성도이다.

도 4는 본 발명에 의한 컴퓨터 시스템의 네트워크 접속부 및 바이오스의 구성도이다.

도 5는 본 발명에 의한 컴퓨터 시스템의 패스워드 확인을 통한 원격 웨이크 업 과정을 도시한 흐름도이다.

도 6은 본 발명에 의한 컴퓨터 시스템의 패킷 확인을 통한 원격 웨이크 업 과정을 도시한 흐름도이다.

도 7은 본 발명에 의한 컴퓨터 시스템의 패스워드 및 패킷 확인을 통한 원격 웨이크 업 과정을 도시한 흐름도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 컴퓨터 시스템에 관한 것으로서, 특히 원격지 웨이크 업 기능을 갖는 컴퓨터 시스템 및 컴퓨터 시스템의 원격 웨이크 업 방법에 관한 것이다.

도 1에 의하면, 다수의 컴퓨터 시스템들이 네트워크(100)에 의해 연결되어 있다. 통상적으로, 네트워크(100)에 접속된 컴퓨터 시스템들은 사용되고 있지 않는 경우에는 컴퓨터 시스템에 구비된 전원 관리 장치(Power Management Unit)에 의해 중지(Suspend) 상태를 유지하고 있다.

한편, 수퍼바이저(110)는 전체 시스템의 관리를 위해 또는 소프트웨어를 업그레이드하거나, 유지 보수를 하기 위해 네트워크(100)에 접속된 다른 컴퓨터 시스템들에 엑세스할 필요가 있다. 이때, 수퍼바이저는 먼저 중지 상태에 있는 타겟 컴퓨터 시스템(120, 130, 140)을 웨이크 업하여야 한다.

중지 상태에 있는 컴퓨터 시스템을 원격지에 있는 수퍼바이저가 웨이크 업하는 종래의 방법은 도 2와 같다.

수퍼바이저가 타겟 컴퓨터 시스템이 웨이크 업하도록 지시하는 매직 패킷을 생성하고, 타겟 컴퓨터 시스템은 네트워크를 통해 매직 패킷을 수신한다(200 단계).

타겟 컴퓨터 시스템은 수신된 패킷에 포함된 네트워크 주소가 자신의 네트워크 주소와 일치하면 웨이크 업 제어신호를 생성하여 타겟 컴퓨터 시스템에 구비된 전원 관리 장치로 보낸다(210 단계). 만약, 주소가 일치하지 않으면, 그 매직 패킷을 버린다(220 단계).

전원 관리 장치가 웨이크 업 제어신호를 받으면, 타겟 컴퓨터 시스템의 중앙처리장치에 전원이 공급되고, 바이오스(Basic Input/Output System : BIOS)가 시스템 부팅 과정을 수행하여, 운영체제를 로드하게 된다(230, 240 단계).

그런데, 종래의 기술에 의하면 수퍼바이저가 아닌 컴퓨터 시스템에서도 매직 패킷을 생성하여 중지 상태에 있는 다른 컴퓨터 시스템에 엑세스할 수 있으므로, 악의의 사용자가 네트워크에 의해 연결된 다른 컴퓨터에 저장된 정보를 인출하거나, 다른 컴퓨터를 손상시킬 수 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기의 문제점을 해결하기 위하여 창작된 것으로서, 정당한 수퍼바이저로부터 수신된 매직 패킷에 의해서만 웨이크 업되는 컴퓨터 시스템 및 그 컴퓨터 시스템의 원격 웨이크 업 방법을 제공함을 그 목적으로 한다.

발명의 구성 및 작용

상기의 목적을 달성하기 위하여, 본 발명에 의한 트랜스포머, 물리적 계층부 및 네트워크 제어기를 포함하는 네트워크 접속장치를 구비하여 네트워크에 접속된 컴퓨터 시스템은 네트워크 주소 및 패스워드를 포함한 네트워크 정보를 저장한 네트워크 정보 저장부; 및 상기 물리적 계층부를 통해 매직 패킷을 수신하고 상기 매직 패킷에 포함된 네트워크 주소 및 패스

워드와 상기 네트워크 정보 저장부에 저장된 네트워크 주소 및 패스워드를 비교하여, 네트워크 주소와 패스워드가 일치하는 경우에만 상기 컴퓨터 시스템이 구비한 전원 관리 장치에 웨이크 업 제어신호를 전달하는 매직 패킷 제어기를 포함하고, 상기 웨이크 업 제어신호에 의해 중지 상태에 있던 시스템이 다시 부팅됨을 특징으로 한다.

상기의 다른 목적을 달성하기 위하여, 본 발명에 의한 컴퓨터 시스템의 원격 웨이크 업 방법은 (a) 네트워크 상에서 매직 패킷을 수신하는 단계; (b) 상기 매직 패킷에 포함된 네트워크 주소를 확인하는 단계; (c) 상기 매직 패킷에 포함된 패스워드를 확인하는 단계; (d) 웨이크 업 제어신호를 생성하는 단계; 및 (e) 바이오스에 의해 시스템 부팅을 수행하는 단계를 포함하고, 상기 (b)단계, 상기 (c)단계에서 확인이 되지 않는 경우에는 웨이크 업을 중단하는 것을 특징으로 한다.

상기의 또 다른 목적을 달성하기 위하여, 본 발명에 의한 컴퓨터 시스템의 원격 웨이크 업 방법은 (a) 네트워크 상에서 매직 패킷을 수신하는 단계; (b) 상기 매직 패킷에 포함된 네트워크 주소를 확인하는 단계; (c) 바이오스에 의해 POST 과정을 수행하는 단계; (d) 상기 매직 패킷에 포함된 주소에 의해 식별된 수퍼바이저 시스템으로 확인요청 패킷을 전송하는 단계; (e) 상기 수퍼바이저 시스템으로부터 확인 패킷을 수신하는 단계; (f) 상기 확인 패킷을 확인하는 단계; 및 (g) 운영체제를 로드하여 수행하는 단계를 포함하고, 상기 (b)단계, 상기 (f)단계에서 확인이 되지 않는 경우에는 웨이크 업을 중단하는 것을 특징으로 한다.

이하에서 첨부된 도면을 참조하여 본 발명을 상세히 설명한다.

도 3에 의하면, 본 발명의 일실시예로서의 원격 웨이크 업 기능을 갖는 컴퓨터 시스템은 트랜스포머(320), 물리적 계층부(310) 및 네트워크 제어기(300)를 포함하는 네트워크 접속장치뿐만 아니라 매직 패킷 제어기(330) 및 네트워크 정보 저장부(340)를 포함하여 구성된다.

네트워크 정보 저장부(340)는 네트워크 주소 및 패스워드를 포함한 네트워크 정보를 저장하고, EEPROM(Electrically Erasable and Programmable ROM)으로 구현됨이 바람직하다.

매직 패킷 제어부(330)는 물리적 계층부(310)를 통해 매직 패킷(a)을 수신하고, 상기 매직 패킷에 포함된 네트워크 주소 및 패스워드와 네트워크 정보 저장부(340)에 저장된 네트워크 주소 및 패스워드를 비교하여, 네트워크 주소와 패스워드가 일치하는 경우에만 전원 관리 장치에 웨이크 업 제어신호를 전달한다.

도 3에서 참조 번호 20에 의해 표시된 구성요소들은 컴퓨터 시스템이 중지 상태에 있더라도 스위칭모드전원공급기(Switching mode power supply : 이하에서 SMPS라 한다)로부터 전원을 공급받는다. 웨이크 업 제어신호에 의해 컴퓨터 시스템이 정상 상태로 바뀌면, 네트워크 제어기(300)는 매직 패킷 제어기(330)를 경유하여 네트워크 정보 저장부(340)에 저장된 네트워크 정보(b)를 엑세스하여, 네트워크를 통한 데이터의 송수신을 제어한다.

도 3에서 참조 번호 10에 의해 표시된 구성요소들은 별도의 카드로 구현되거나, 컴퓨터 시스템의 메인 보드에 온보드되어 구현될 수 있다.

도 4에 의하면, 본 발명의 다른 일실시예로서의 원격 웨이크 업 기능을 갖는 컴퓨터 시스템은 트랜스포머(420), 물리적 계층부(410) 및 네트워크 제어기(400)를 포함하는 네트워크 접속장치뿐만 아니라 매직 패킷 제어기(430), 네트워크 정보 저장부(440) 및 매직 패킷 확인부(463)를 구비한 바이오스(460)를 포함하여 구성된다.

네트워크 정보 저장부(440)는 네트워크 주소 및 패스워드를 포함한 네트워크 정보를 저장하고, EEPROM으로 구현됨이 바람직하다.

메직 패킷 제어부(430)는 물리적 계층부(410)를 통해 매직 패킷(c)을 수신하고, 상기 매직 패킷에 포함된 네트워크 주소 및 패스워드와 네트워크 정보 저장부(440)에 저장된 네트워크 주소 및 패스워드를 비교하여, 네트워크 주소와 패스워드가 일치하는 경우에만 전원 관리 장치에 웨이크 업 제어신호를 전달한다.

바이오스(460)는 통상의 전원인가후 자가검사(Power On Self Test : 이하에서 POST라 한다) 수행부(462) 및 인터럽트를 처리하는 루틴을 포함하는 인터럽트 핸들러(464) 뿐만 아니라, 웨이크 업 제어신호에 의해 컴퓨터 시스템이 부팅될 때, 매직 패킷을 전송한 수퍼바이저 시스템에 확인을 요청하는 확인요청 패킷을 전송하고, 수퍼바이저 시스템으로부터 확인 패킷을 받은 경우에만 시스템 부팅 과정을 계속 수행하는 매직 패킷 확인부를 POST 수행부(462) 내에 구비한다.

바이오스(460)는 ISA(Industry Standard Architecture) 버스에 접속되고, ISA 버스는 PCI to ISA 브릿지(450)를 통해 PCI(Peripheral Component Interconnect) 버스와 상호 접속된다.

도 4에서 참조 번호 40에 의해 표시된 구성요소들은 컴퓨터 시스템이 중지 상태에 있더라도 SMPS로부터 전원을 공급받는다. 웨이크 업 제어신호에 의해 컴퓨터 시스템이 정상 상태로 바뀌면, 네트워크 제어기(400)는 매직 패킷 제어기(430)를 경유하여 네트워크 정보 저장부(440)에 저장된 네트워크 정보(d)를 엑세스하여, 네트워크를 통한 데이터의 송수신을 제어한다.

도 5에 의하면, 본 발명의 일실시예로서의 컴퓨터 시스템의 웨이크 업 과정은 다음과 같다.

먼저, 도 3의 물리적 계층부(310)는 네트워크 주소 및 패스워드가 포함된 매직 패킷을 네트워크 상에서 수신하여, 매직 패킷 제어기(330)로 전달한다(500 단계).

매직 패킷 제어기(330)는 수신된 매직 패킷에 포함된 네트워크 주소 뿐만 아니라 패스워드를 네트워크 정보 저장부(340)에 저장된 네트워크 주소 및 패스워드와 비교하여 일치하는지 여부를 확인한다(510, 530 단계). 이때, 일치하지 않는 경우에는 매직 패킷을 버리고, 웨이크 업은 중단된다(520 단계).

매직 패킷 제어기(330)는 네트워크 주소 및 패스워드가 일치하면, 웨이크 업 제어신호를 생성하여 전원 관리 장치에 보낸다. 그러면, 전원 관리 장치에 의해 컴퓨터 시스템은 중지 상태에서 정상 상태로 바뀌고, 중앙처리장치에 전원이 공급되어 바이오스에 의해 시스템이 부팅되고, 운영체제가 로드되어 수행된다(540, 550 단계).

도 6에 의하면, 본 발명의 다른 일실시예로서의 컴퓨터 시스템의 웨이크 업 과정은 다음과 같다.

먼저, 도 4의 물리적 계층부(410)는 네트워크 주소 및 패스워드가 포함된 매직 패킷을 네트워크 상에서 수신하여, 매직 패킷 제어기(430)로 전달한다(600 단계).

매직 패킷 제어기(430)는 수신된 매직 패킷에 포함된 네트워크 주소를 네트워크 정보 저장부(440)에 저장된 네트워크 주소와 비교하여 일치하는지 여부를 확인한다(610 단계). 이때, 일치하지 않는 경우에는 매직 패킷을 버리고, 웨이크 업은 중단된다(620 단계).

매직 패킷 제어기(430)는 네트워크 주소가 일치하면, 웨이크 업 제어신호를 생성하여 전원 관리 장치에 보낸다. 그러면, 전원 관리 장치에 의해 컴퓨터 시스템은 중지 상태에서 정상 상태로 바뀌고, 중앙처리장치에 전원이 공급되어 바이오스의 POST 수행부(462)에 의해 POST 과정이 수행된다(630 단계).

POST 과정 중 매직 패킷 확인부(463)는 매직 패킷에 포함된 주소에 의해 식별된 수퍼바이저 시스템으로 확인요청 패킷을 전송한다(640 단계). 확인요청 패킷은 네트워크 제어부(400), 물리적 계층부(410) 및 트랜스포머(420)를 경유하여 네트워크를 통해 전달된다.

소정의 시간이 경과한 후, 매직 패킷 확인부(463)는 트랜스포머(420), 물리적 계층부(410) 및 네트워크 제어부(400)를 통해 수퍼바이저 시스템으로부터의 확인 패킷을 수신한다(650 단계). 이때, 확인 요청 패킷에는 소정의 방법에 의해 생성된 난수가 포함되고, 확인 패킷은 상기 난수와 소정의 암호 생성 함수에 의해 생성된 암호가 포함된다.

매직 패킷 확인부(463)는 확인 패킷에 포함된 암호와 상기 난수 및 수퍼바이저에 포함된 암호 생성 함수와 동일한 암호 생성 함수에 의해 생성된 암호를 비교한다(660 단계). 이때, 암호가 일치하지 않으면, 매직 패킷을 버리고 컴퓨터 시스템의 웨이크 업 과정을 중단한다(620 단계).

암호가 일치하면, 운영체제가 로드되어 수행된다(670 단계).

도 7에 의하면, 본 발명의 또 다른 일실시예로서의 컴퓨터 시스템의 웨이크 업 과정은 다음과 같다.

먼저, 도 4의 물리적 계층부(410)는 네트워크 주소 및 패스워드가 포함된 매직 패킷을 네트워크 상에서 수신하여, 매직 패킷 제어기(430)로 전달한다(700 단계).

매직 패킷 제어기(430)는 수신된 매직 패킷에 포함된 네트워크 주소 뿐만 아니라 패스워드를 네트워크 정보 저장부(440)에 저장된 네트워크 주소 및 패스워드와 비교하여 일치하는지 여부를 확인한다(710 단계).

이하의 과정들(720 단계 내지 770 단계)은 도 6의 과정들(620 단계 내지 670 단계)과 동일하다. 따라서, 매직 패킷 제어부(430)에서의 패스워드에 의한 확인 과정과 바이오스(460)에 구비된 매직 패킷 확인부(463)에 의한 확인 패킷의 확인 등 2단계의 확인을 통해 정당한 수퍼바이저인지 여부를 구분한다.

발명의 효과

본 발명에 의하면, 네트워크를 통해 다른 컴퓨터 시스템을 원격 웨이크 업할 때, 정당한 수퍼바이저에 의한 웨이크 업인지 여부를 확인함으로써 악의의 사용자로부터 컴퓨터 시스템의 정보가 유출되거나, 컴퓨터 시스템이 손상되는 것을 방지할 수 있다.

(57) 청구의 범위

청구항 1.

트랜스포머, 물리적 계층부 및 네트워크 제어기를 포함하는 네트워크 접속장치를 구비하여 네트워크에 접속된 컴퓨터 시스템에 있어서,

네트워크 주소 및 패스워드를 포함한 네트워크 정보를 저장한 네트워크 정보 저장부;

상기 물리적 계층부를 통해 매직 패킷을 수신하고 상기 매직 패킷에 포함된 네트워크 주소 및 패스워드와 상기 네트워크 정보 저장부에 저장된 네트워크 주소 및 패스워드를 비교하여, 네트워크 주소 및 패스워드가 일치하는 경우에만 상기 컴퓨터 시스템이 구비한 전원 관리 장치에 웨이크 업 제어신호를 전달하는 매직 패킷 제어기; 및

상기 웨이크 업 제어신호에 의해 상기 컴퓨터 시스템이 부팅될 때, 상기 매직 패킷을 전송한 수퍼바이저 시스템에 확인을 요청하는 확인요청 패킷을 전송하고, 수퍼바이저 시스템으로부터 확인 패킷을 받은 경우에만 시스템 부팅 과정을 계속 수행하는 매직 패킷 확인부를 구비한 바이오스를 포함하고,

상기 웨이크 업 제어신호에 의해 중지 상태에 있던 시스템이 다시 부팅됨을 특징으로 하는 네트워크 접속용 컴퓨터 시스템.

청구항 2.

(a) 네트워크 상에서 매직 패킷을 수신하는 단계;

(b) 상기 매직 패킷에 포함된 네트워크 주소를 확인하는 단계;

(c) 상기 매직 패킷에 포함된 주소에 의해 식별된 수퍼바이저 시스템으로 확인요청 패킷을 전송하는 단계;

(d) 상기 수퍼바이저 시스템으로부터 확인 패킷을 수신하는 단계;

(e) 상기 확인 패킷을 확인하는 단계; 및

(f) 운영체제를 로드하여 시스템 부팅을 수행하는 단계를 포함하고,

상기 (b)단계, 상기 (e)단계에서 확인이 되지 않는 경우에는 웨이크 업을 중단하는 것을 특징으로 하는 네트워크에 접속된 컴퓨터 시스템의 원격 웨이크 업 방법.

청구항 3.

제2항에 있어서, 상기 (b)단계는

상기 매직 패킷에 포함된 패스워드를 확인하는 과정을 더 포함하는 것을 특징으로 하는 네트워크에 접속된 컴퓨터 시스템의 원격 웨이크 업 방법.

청구항 4.

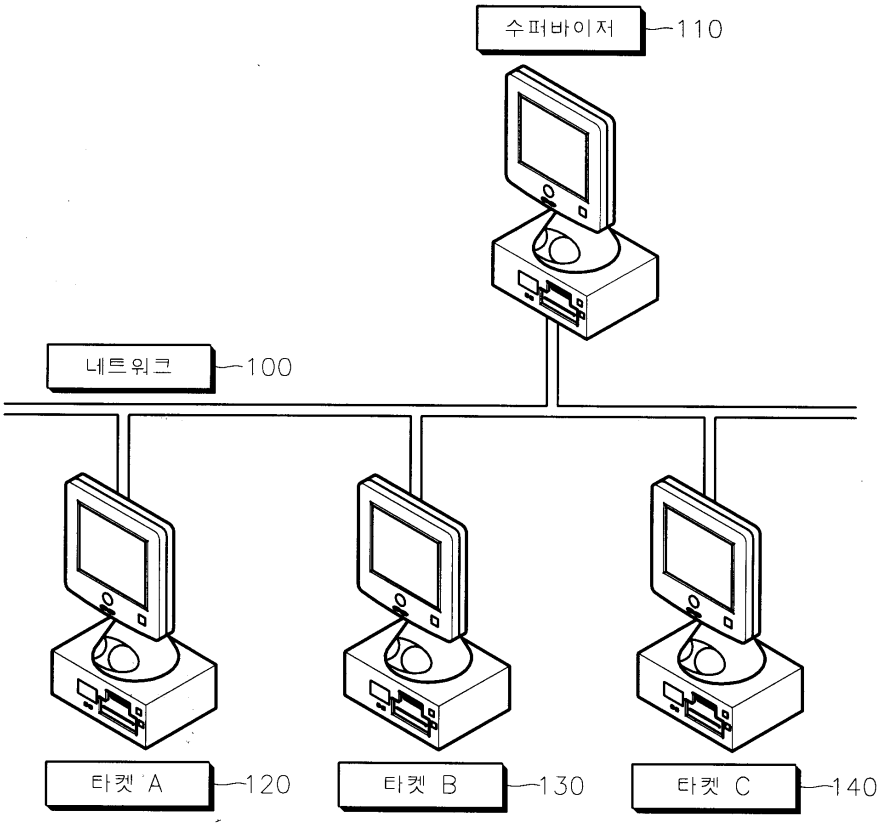
제2항에 있어서, 상기 확인요청 패킷은

난수를 포함하고,

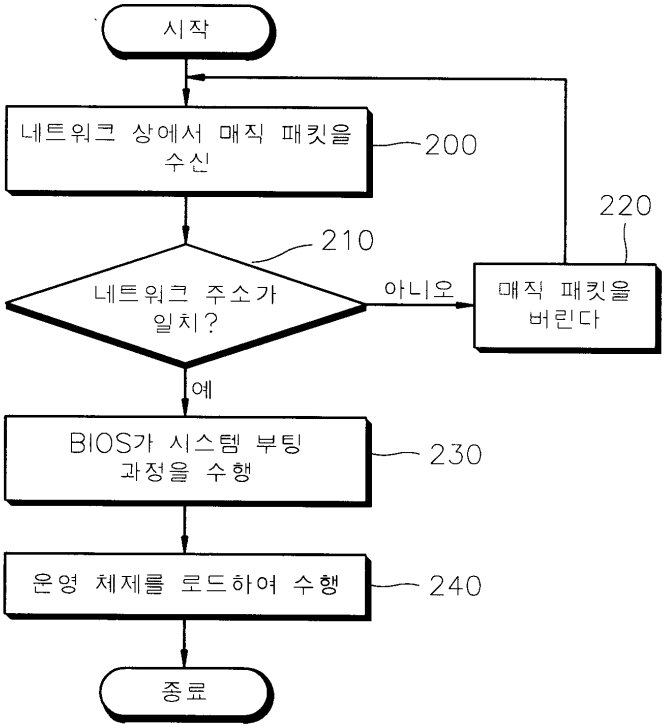
상기 확인 패킷은 상기 난수와 소정의 암호 생성 함수에 의해 생성된 암호를 포함하는 것을 특징으로 하는 네트워크에 접속된 컴퓨터 시스템의 원격 웨이크 업 방법.

도면

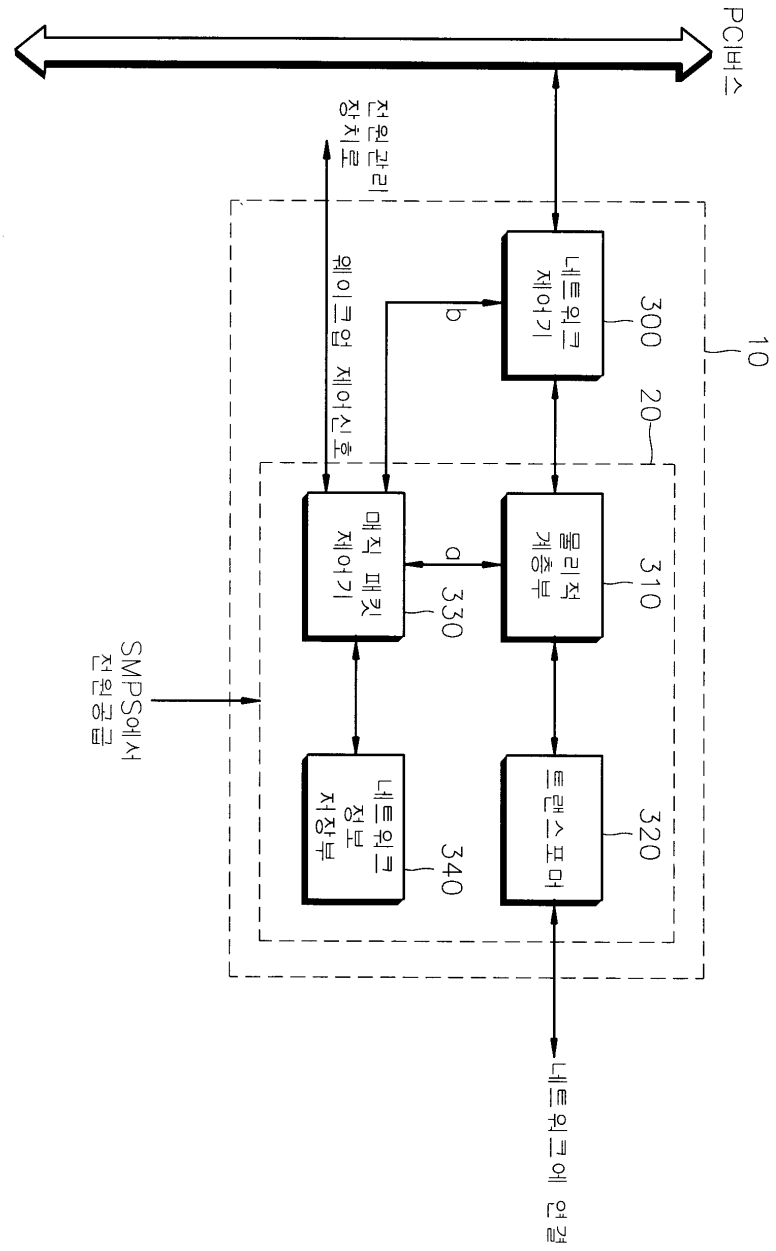
도면1



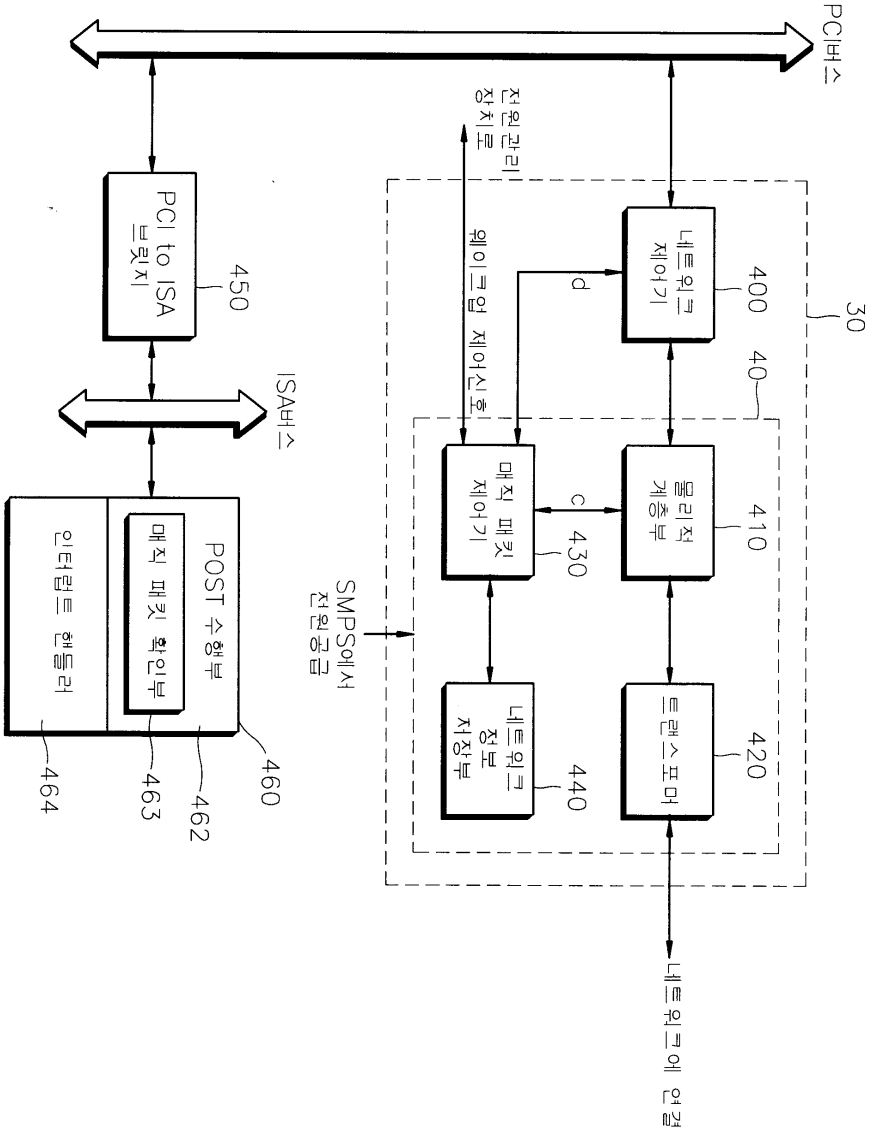
도면2


시작
네트워크 상에서 매직 패킷을 수신
200
210
네트워크 주소가 일치?
아니오
220
매직 패킷을 버린다
예
BIOS가 시스템 부팅 과정을 수행
230
운영 체제를 로드하여 수행
240
종료

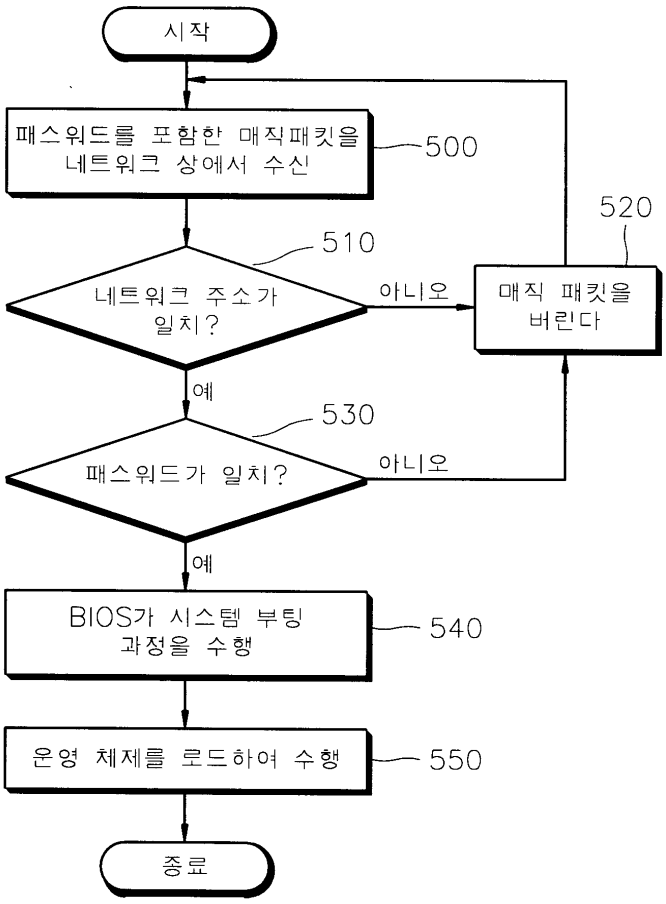
도면3


PC버스
전원관리 장치로
웨이크업 제어신호
네트워크 제어기
300
10
20
b
매직 패킷 제어기
a
330
물리적 계층부
310
SMPS에서 전원공급
네트워크 정보 저장부
340
트랜스포머
320
네트워크에 연결

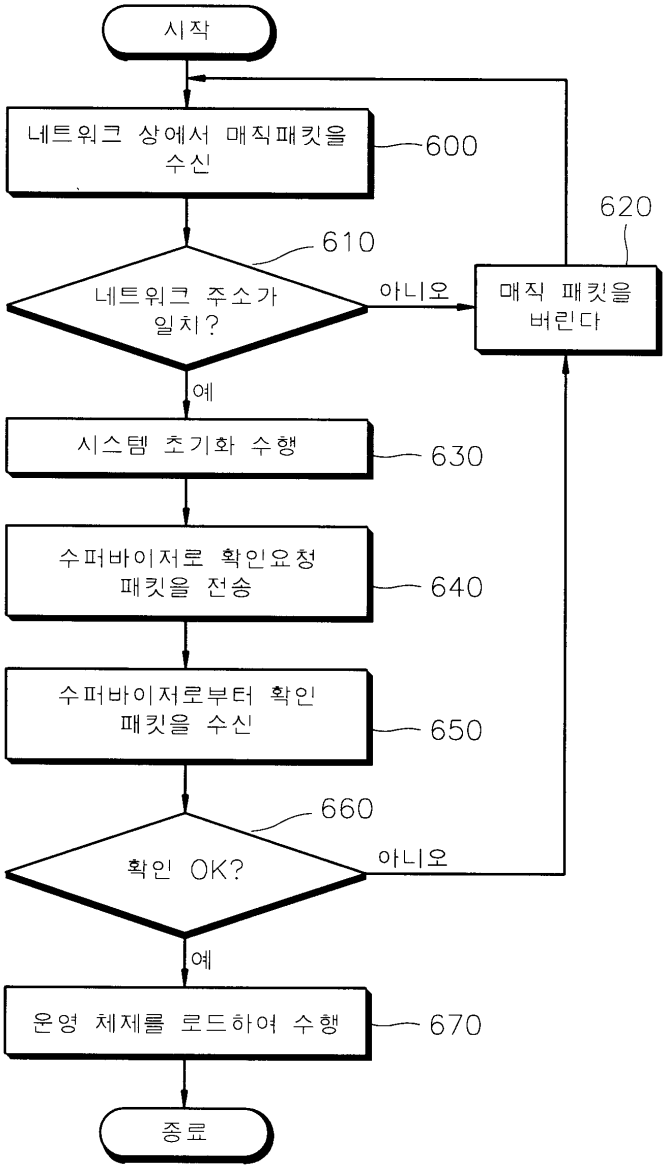
도면4


PCI버스
전원관리 장치로
웨이크업 제어신호
네트워크 제어기
400
30
40
d
PCI to ISA 브릿지
450
ISA버스
매직 패킷 제어기
c
430
물리적 계층부
410
SMPS에서 전원공급
네트워크 정보 저장부
440
트랜스포머
420
네트워크에 연결
POST 수행부
매직 패킷 확인부
463
462
460
인터럽트 핸들러
464

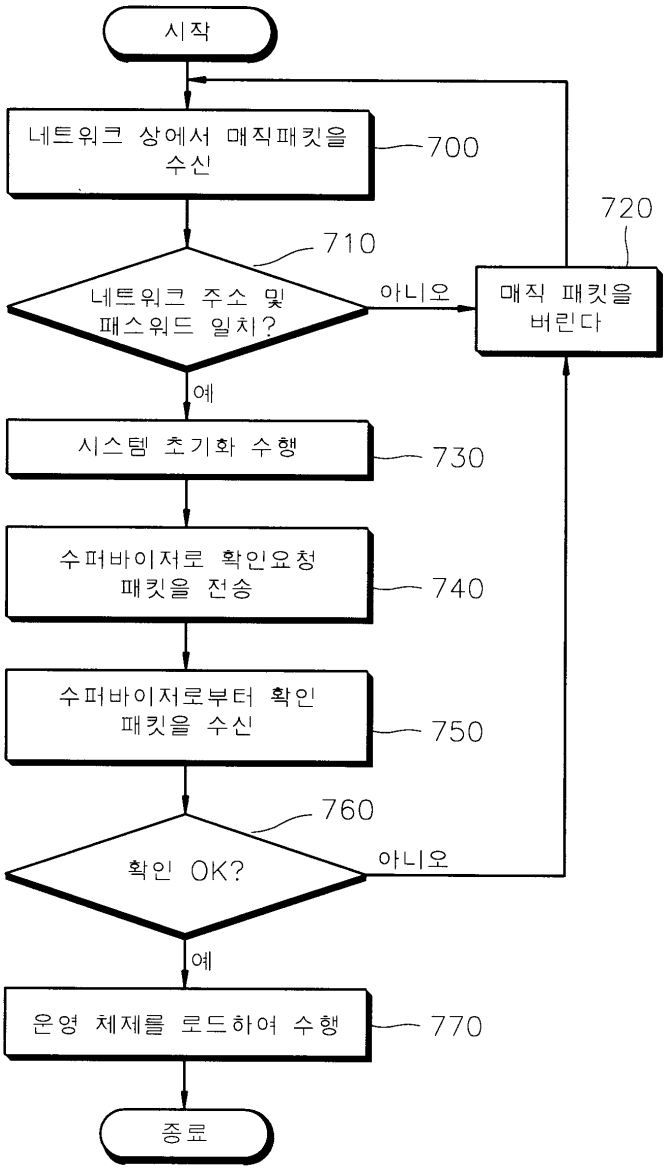
도면5


시작
패스워드를 포함한 매직패킷을 네트워크 상에서 수신
500
네트워크 주소가 일치?
510
아니오
매직 패킷을 버린다
520
예
패스워드가 일치?
530
아니오
예
BIOS가 시스템 부팅 과정을 수행
540
운영 체제를 로드하여 수행
550
종료

도면6


시작
네트워크 상에서 매직패킷을 수신
600
610
네트워크 주소가 일치?
아니오
620
매직 패킷을 버린다
예
시스템 초기화 수행
630
수퍼바이저로 확인요청 패킷을 전송
640
수퍼바이저로부터 확인 패킷을 수신
650
660
확인 OK?
아니오
예
운영 체제를 로드하여 수행
670
종료

도면7


시작
네트워크 상에서 매직패킷을 수신
700
710
네트워크 주소 및 패스워드 일치?
아니오
720
매직 패킷을 버린다
예
시스템 초기화 수행
730
수퍼바이저로 확인요청 패킷을 전송
740
수퍼바이저로부터 확인 패킷을 수신
750
760
확인 OK?
아니오
예
운영 체제를 로드하여 수행
770
종료