(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101741636 A
(43)申请公布日 2010.06.16

(21)申请号 200910218054.4

(22)申请日 2009.12.22

(71)申请人 中国科学院长春光学精密机械与物理研究所
地址 130033 吉林省长春市东南湖大路3888号

(72)发明人 杨怀江 隋永新 章明朝 李珮玥 刘超群

(74)专利代理机构 长春菁华专利商标代理事务所 22210
代理人 刘树清

(51)Int.Cl.
*H04L 12/26*(2006.01)
*H04L 29/06*(2006.01)

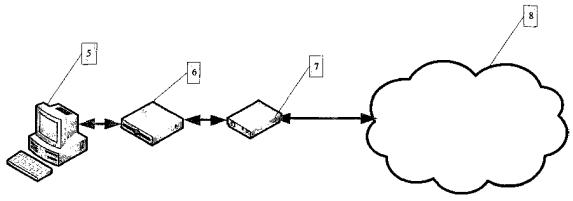
权利要求书 1 页 说明书 4 页 附图 3 页

(54)发明名称

一种采用芯片TMS320F2812的计算机网络监控系统

(57)摘要

一种采用芯片TMS320F2812的计算机网络监控系统，属于计算机网络技术领域涉及的一种网络监控系统，本发明要解决的技术问题是：提供一种采用芯片TMS320F2812的计算机网络监控系统。解决的技术方案为：包括个人计算机5、计算机网络监管系统6、互联网接口7(如ADSL调制解调器)、互联网8；将计算机网络监管系统6的输入端和个人计算机5连接，输出端与互联网接口7的输入端连接，互联网接口7的输出端与互联网8连接。本发明能保证网络数据正常流通，提供身份认证功能，可控制上网时间，记录访问网址以及提供黑名单功能。




CN 101741636 A

1. 一种采用芯片 TMS320F2812 的计算机网络监控系统，包括个人计算机 (5)、互联网接口 (7)、互联网 (8)；其特征在于还包括计算机网络监管系统 (6)，将计算机网络监管系统 (6) 的输入端和个人计算机 (5) 连接，输出端与互联网接口 (7) 的输入端连接，互联网接口 (7) 的输出端与互联网 (8) 连接。

2. 按权利要求 1 所述的一种采用芯片 TMS320F2812 的计算机网络监控系统；其特征在于计算机网络监管系统 (6) 包括第一网络接口芯片 DM9000A(9)、主控芯片 TMS320F2812(10)、第二网络接口芯片 DM9000A(11)、实时时钟控制芯片 DS1305(12)、闪存芯片 S29GL064N(13)；第一网络接口芯片 DM9000A(9) 和第二网络接口芯片 DM9000A(11) 都通过数据总线连接到主控芯片 TMS320F2812(10) 上，同时采用主控芯片 TMS320F2812(10) 的管脚 ZCS01# 作为片选信号源，在地址总线的控制下将两个网络接口芯片的地址映射到主控芯片 TMS320F2812(10) 的地址空间上；实时时钟芯片 DS1305(12) 通过串行外围接口连接到主控芯片 TMS320F2812(10) 上；闪存芯片 S29GL064N(13) 通过数据总线和地址总线连接到主控芯片 TMS320F2812(10) 上，同时采用主控芯片 TMS320F2812(10) 的管脚 ZCS67# 作为片选信号源；计算机网络监管系统 6 在正常工作时，将要上网的个人计算机 (5) 的 IP 地址映射到第二网络接口芯片 DM9000A(11) 上，并为第一网络接口芯片 DM9000A(9) 设值一个虚拟的 IP 地址；第一网络接口芯片 DM9000A(9) 通过网线接收个人计算机 (5) 发送的网络数据包，按照网络协议封包格式对网络数据包进行解封后，通过数据总线将应用层数据传送给主控芯片 TMS320F2812(10) 进行处理，需要处理的应用层数据有两种：一是自定义协议，用来发送自定义的各种命令和控制信息；另一个是超文本传输协议，包含用户上网时的请求信息；网路数据包的封装格式是按照传输控制协议 / 网际协议设计的，传输控制协议 / 网际协议是链路层、网络层、运输层和应用层上不同层次的多个协议的组合；在本设计中使用到的协议包括：链路层的电气和电子工程师协会 802 协议，网络层的网际协议，运输层的传输控制协议和用户数据报协议，应用层的超文本传输和自定义协议；在应用层的自定义协议中，各个字段的意义定义为：类型字段，定义发送数据包的类型，根据该字段区别使用者的不同操作，如检测设备，密码验证，查询网络状态等；握手字段，每次传输过程中的握手字段，0x6F6B 表示传输正确，0x0000 表示传输过程有错误；数据字段，用来传输不同操作中所包含的数据包，长度固定为 1024 字节；校验字段，自定义协议数据包的循环冗余码校验。

# 一种采用芯片 TMS320F2812 的计算机网络监控系统

## 技术领域

[0001] 本发明属于计算机网络技术领域，涉及一种采用芯片 TMS320F2812 的计算机网络监控系统，具体地说涉及一种通过分析计算机网络数据包以及设置上网时间等技术手段对上网行为进行监控的装置。

## 背景技术

[0002] 随着社会的进步与经济的发展，因特网的兴起使人类正迈向网络社会的新时代，其带来的便利是有目共睹的：网上聊天、网络新闻、网上购物等都极大地丰富了人们的生活和视野。但是，因特网上的信息污染也日益严重，色情淫秽，恐怖暴力，反政府及种族歧视等非法信息充斥其中。有的网络用户因缺乏自身约束力很容易受到网络的危害，沉迷于网络。因此建立一个完善的网络监管系统，对网络用户，特别是针对青少年进行适当的引导和敦促是很有必要的。这样即可以有效地利用网络资源，又防止了用户过度地沉迷于网络。

[0003] 现有的网络监管系统主要是通过软件来实现的，与本发明最为接近的已有技术是普通的常用网络监管系统。如图 1 所示，在个人计算机 1 上安装了用于网络监管的软件 2，个人计算机 1 通过各种网络接口 3（如调制解调器）连接到互联网 4 上，网络监管软件 2 对个人计算机 1 的上网数据进行监听和管理。这种网络监管系统存在的主要问题是：其实现方式网络用户很容易通过卸载，屏蔽或是简单地退出软件，终止软件工作进程等手段绕过监管系统，无法达到网络监控的目的。

## 发明内容

[0004] 为了克服已有技术存在的缺陷，本发明的目的在于提供一种用户无法绕过的，可以严格控制上网时间，拒绝访问黑名单上的网址以及建立网络监管日志的适用于家庭，学校等场所的采用芯片

[0005] TMS320F2812 的嵌入式网络监管系统。

[0006] 本发明要解决的技术问题是：提供一种采用芯片 TMS320F2812 的计算机网络监控系统，解决技术问题的技术方案如图 2 所示，包括个人计算机 5、计算机网络监管系统 6、互联网接口 7（如 ADSL 调制解调器）、互联网 8；将计算机网络监管系统 6 的输入端和个人计算机 5 连接，输出端与互联网接口 7 的输入端连接，互联网接口 7 的输出端与互联网 8 连接。计算机网络监管系统 6 为自行设计的嵌入式设备，硬件结构如图 3 所示，包括第一网络接口芯片 DM9000A 9、主控芯片 TMS320F281210、第二网络接口芯片 DM9000A 11、实时时钟控制芯片 (RTC 芯片)DS1305 12、闪存芯片 S29GL064N 13；第一网络接口芯片 DM9000A 9 和第二网络接口芯片 DM9000A 11 都通过数据总线连接到主控芯片 TMS320F2812 10 上，同时采用主控芯片 TMS320F281210 的管脚 ZCS01# 作为片选信号源，在地址总线的控制下将两个网络接口芯片的地址映射到主控芯片 TMS320F2812 10 的地址空间上；实时时钟芯片 DS1305 12 通过串行外围接口 (SPI) 连接到主控芯片 TMS320F2812 10 上；闪存芯片 S29GL064N 13 通过数据总线和地址总线连接到主控芯片 TMS320F2812 10 上，同时采用主控芯片 TMS320F2812

10 的管脚 ZCS67# 作为片选信号源 ;

[0007] 计算机网络监管系统 6 在正常工作时,将要上网的个人计算机 5 的 IP( 网际协议 ) 地址映射到第二网络接口芯片 DM9000A 11 上,并为第一网络接口芯片 DM9000A 9 设值一个虚拟的 IP( 网际协议 ) 地址 ;第一网络接口芯片 DM9000A 9 通过网线接收个人计算机 5 发送的网络数据包,按照图 4 所示的网络协议封包格式对网络数据包进行解封后,通过数据总线将应用层数据传送给主控芯片 TMS320F281210 进行处理,需要处理的应用层数据有两种 :一是自定义协议 (CAFA 协议 ),用来发送自定义的各种命令和控制信息 ;另一个是超文本传输协议 (HTTP),包含用户上网时的请求信息 ;

[0008] 网路数据包的封装格式是按照传输控制协议 / 网际协议 (TCP/IP 协议 ) 设计的,传输控制协议 / 网际协议 (TCP/IP 协议 ) 是链路层、网络层、运输层和应用层上不同层次的多个协议的组合 ;在本设计中使用到的协议包括 :链路层的电气和电子工程师协会 802 协议 (IEEE802 协议 ),网络层的网际协议 (IP 协议 ),运输层的传输控制协议 (TCP 协议 ) 和用户数据报协议 (UDP 协议 ),应用层的超文本传输 (HTTP 协议 ) 和自定义协议 (CAFA 协议 ) ;

[0009] 在应用层的自定义协议中,各个字段的意义定义为 :

[0010] a) 类型字段 (STYLE) :定义发送数据包的类型,根据该字段区别使用者的不同操作 ( 检测设备,密码验证,查询网络状态等 ) ;

[0011] b) 握手字段 (ACK) :每次传输过程中的握手字段,0x6F6B 表示传输正确,0x0000 表示传输过程有错误 ;

[0012] c) 数据字段 (DATA) :用来传输不同操作中所包含的数据包,长度固定为 1024 字节 ;

[0013] d) 校验字段 (CRC) :自定义协议数据包的循环冗余码 (CRC) 校验。

[0014] 本发明的工作原理说明 :本发明设计的软件由两部分组成,安装在个人计算机 5 上的应用层软件和存放在主控芯片 TMS320F2812 10 内的嵌入式软件 ;两部分软件通过自定义协议 (CAFA 协议 ) 进行命令的交互 ;其中应用层软件主要实现用户操作界面的功能,嵌入式软件具体实现了网络监管的功能 ;具体来说 :主控芯片 TMS320F2812 10 分析应用层发送的数据包并截获统一资源定位器数据 (URL,即我们常说的网址 ) 和硬件配置值 ( 管理员密码,上网方式和黑名单 ),并将这些值存储在闪存芯片 S29GL064N 13 上 ;设计时定义一条统一资源定位器数据 (URL) 占用的最大存储空间为 200bits,本发明采用的 64Mbits 闪存芯片 S29GL064N 13 至少可以存放 30 万条统一资源定位器数据 (URL),满足用户使用需求 ;另外,主控芯片 TMS320F2812 10 为实时时钟芯片 DS1305 12 设置时间控制信息,反过来实时时钟芯片 DS1305 12 将为硬件状态提供时间基准,该芯片除了主电源外,另配一节纽扣电池作为备用电源,在硬件断电的情况下保证实时时钟正常工作,这样可以达到上网时间控制的目的 ;主控芯片 TMS320F2812 10 将分析过的且不属于黑名单的网络数据包通过数据总线发送给第二网络接口芯片 DM9000A 11,第二网络接口芯片将此数据按照图 4 所示的网络协议进行封装,然后通过网线发送到互联网 8 上 ;而对于从互联网 8 响应的各种数据不做任何处理,直接发送给个人计算机 5 ;

[0015] 如图 5 所示,本发明有两种不同的操作权限,在保证硬件连接正确的情况下,使用者可以选择登录方式 ;如果选择以普通用户身份登录,则只可以查看上网时间的相关设置 ( 如剩余上网时间或是预设的上网时间段 ),并且根据这些设置判断网络是否连接 ;如果选

择以管理员的身份登录，则需要在验证口令成功的条件下进入管理员操作界面，完成对系统的管理与设置工作，具体功能为：

[0016] 一、时间设置：用来设置硬件时间，以便硬件时间与计算机系统时间同步；

[0017] 二、上网控制方式：采用两种方式对用户上网进行控制，一种是累积时间，即每天有固定的上网时间，但对于何时上网不做控制，在这种方式下只需设置最大上网时间即可，另一种方式是时间段，即每天在固定的时间段内可以上网，需要设置该时间段的起始时间和终止时间；

[0018] 三、查询和保存上网记录：管理员可以查询，删除用户的上网记录以及选择是否保存该上网记录；

[0019] 四、硬件 IP：在用户多网卡或无法自动获取正确的内网 IP 地址时，可以通过手动设置硬件 IP 保证通信正常；

[0020] 五、修改密码：管理员可以通过该项修改登录密码，密码最长为 16 位；

[0021] 六、黑名单：将非法，不健康网站设为黑名单，禁止用户再次访问；使用时，如图 2 所示，将计算机网络监管系统 6 放置在上网个人计算机 5 与互联网端口 7（如 ADSL 调制解调器）之间，对用户访问互联网 8 时的网络数据流进行过滤或阻断，当普通用户上网过程中，只在管理员设定的时间内开放网络功能，同时利用硬件保存已访问的网址和黑名单供管理员实施监督管理；由互联网 8 接收到的数据则不处理，直接根据当前网络状态决定是否发送给个人计算机 5；这些功能通过客户端软件和嵌入式软件共同实现。

[0022] 本发明的积极效果：

[0023] 一、能保证网络数据正常流通

[0024] 所谓桥梁，实现的基本功能当然是连接。本发明具有两个网络端口：第一网络接口和第二网络接口。两个接口分别通过网线连接到个人计算机和互联网端口上，在允许上网的条件下，该系统需保证网络数据的正常流通；

[0025] 二、提供身份认证功能

[0026] 本系统需要为管理员和普通用户设置不同的使用权限。在以普通用户身份登录的过程中，使用者只可以查看硬件的部分设置（如上网时间控制方式，本日剩余上网时间等），而在以管理员身份登录时，除了以上功能外，使用者可以实现对网址的查看与删除、设置硬件信息以及设置登录密码等功能；

[0027] 三、可控制上网时间

[0028] 为了实现管理员不在的情况下严格控制学生的上网时间，管理员需要将时间信息保存在硬件内，通过硬件内部的状态转换实现网络的通断功能；

[0029] 四、记录访问网址

[0030] 由于在计算机上通过软件方式保存的访问网址可以轻易的被删除，所以本系统需要在硬件内完成网络各层协议的解析，并将访问的网址保存在嵌入式存储设备中，只有以管理员的身份登录硬件时才可以操作这些网址。由此实现了管理员对普通用户已访问网站的审计与控制功能，可以有效防止普通用户登陆不良网站；

[0031] 五、提供黑名单功能

[0032] 在嵌入式存储设备中开辟一定大小的空间存放黑名单，管理员可以将非法，不健康网站设置为黑名单，禁止普通用户访问。

## 附图说明

[0033] 图 1 为已有技术系统结构示意图；

[0034] 图 2 为本发明系统结构示意图；

[0035] 图 3 为本发明中计算机网络监管系统 6 的硬件结构示意图；

[0036] 图 4 为本发明中多层次通信协议的方式结构示意图；

[0037] 图 5 为本发明系统软件工作程序流程图。

## 具体实施方式

[0038] 本发明按图2、图3所示的结构实施，其中个人计算机5可以是家庭，学校或是公司内任意一台接入互联网的计算机；计算机网络监管系统 6 是自行研发设计的嵌入式设备；互联网接口 7 是计算机接入互联网的端口，如调制解调器、宽带接口或光纤接口等。

[0039] 计算机网络监管系统 6 在设计时主要采用了四款芯片，其中，主控芯片 10 采用 TI 公司的 TMS320F2812，该芯片属于 DSP2000 系列，具有 150MHz 的 CPU 速度和很强的数据处理能力；第一网络接口芯片 9 和第二网络接口芯片 11 都采用 Davicom 公司生产的 DM9000A，该芯片支持 10/100M 以太网速率，可以与嵌入式微处理器、单片机等以多种方式接口，具有体积小、功耗低、配置灵活、使用简单等特点；实时时钟芯片采用美国 Dallas 公司推出的 DS1305，该芯片是串行接口带警实时时钟，可以用二一十进制码表示实时时钟的秒、分、小时、星期、日、月和年的时间信息，并且自动对小月和闰年的日期进行调整；闪存芯片 13 采用 Spansion 公司推出的一款 64M nor FlashS29GI064N。

[0040] 以上只是对本发明技术方案单一实施例的描述，实现本发明创造有多种形式，本领域的普通技术人员可以根据实际需求做出各种改进。

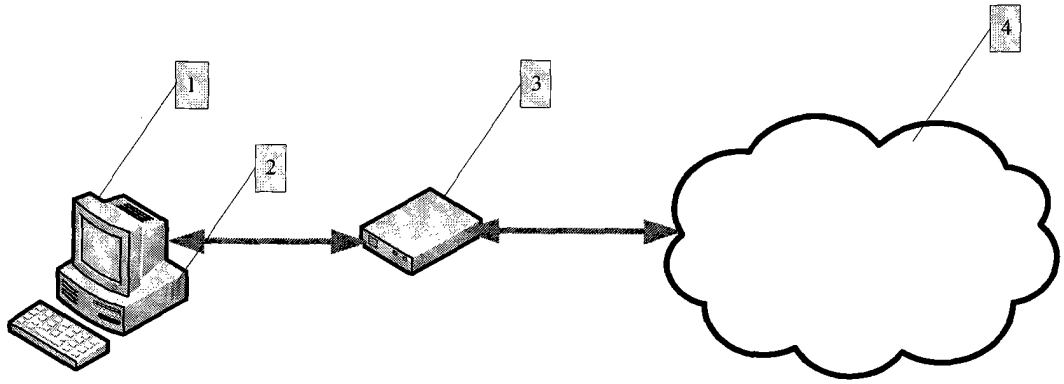



图 1

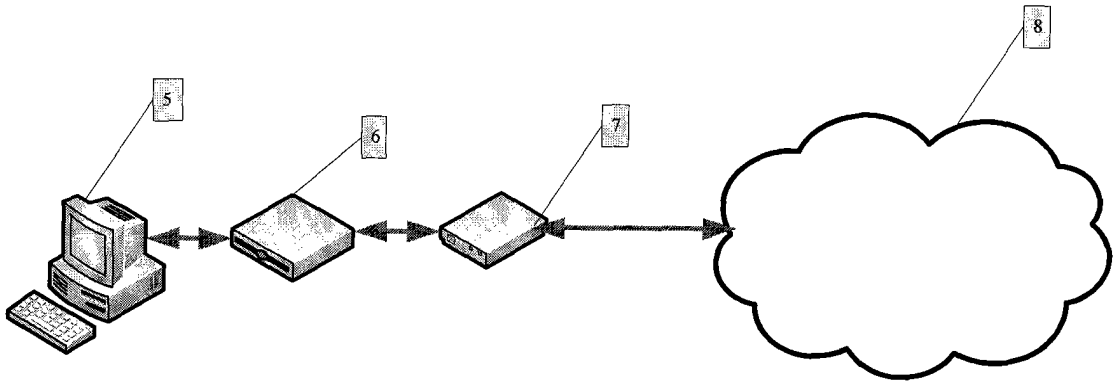



图 2

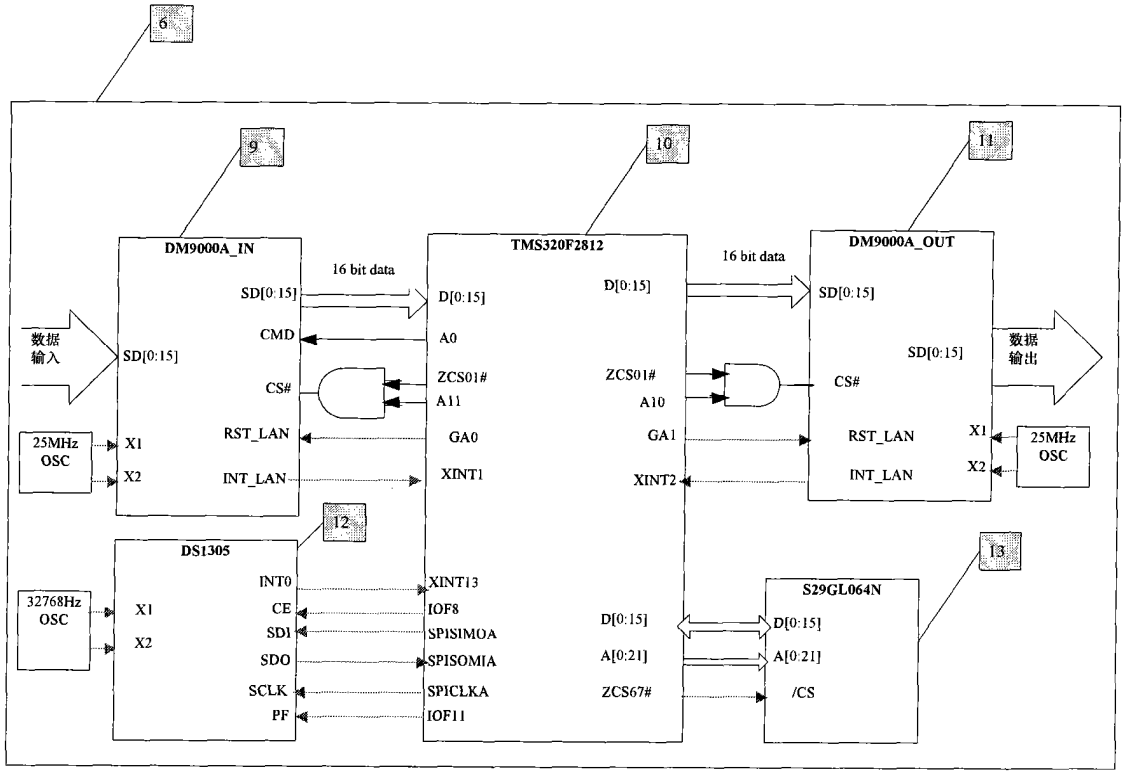

6
9
10
11
DM9000A_IN
TMS320F2812
DM9000A_OUT
16 bit data
16 bit data
SD[0:15]
D[0:15]
D[0:15]
SD[0:15]
数据输入
CMD
A0
SD[0:15]
数据输出
CS#
ZCS01#
A11
ZCS01#
A10
CS#
25MHz OSC
X1
X2
RST_LAN
INT_LAN
GA0
XINT1
GA1
XINT2
RST_LAN
INT_LAN
X1
X2
25MHz OSC
12
13
DS1305
S29GL064N
32768Hz OSC
X1
X2
INT0
CE
SDI
SDO
SCLK
PF
XINT13
IOF8
SPISIMOA
SPISOMIA
SPICLKA
IOF11
D[0:15]
A[0:21]
ZCS67#
D[0:15]
A[0:21]
/CS

图 3

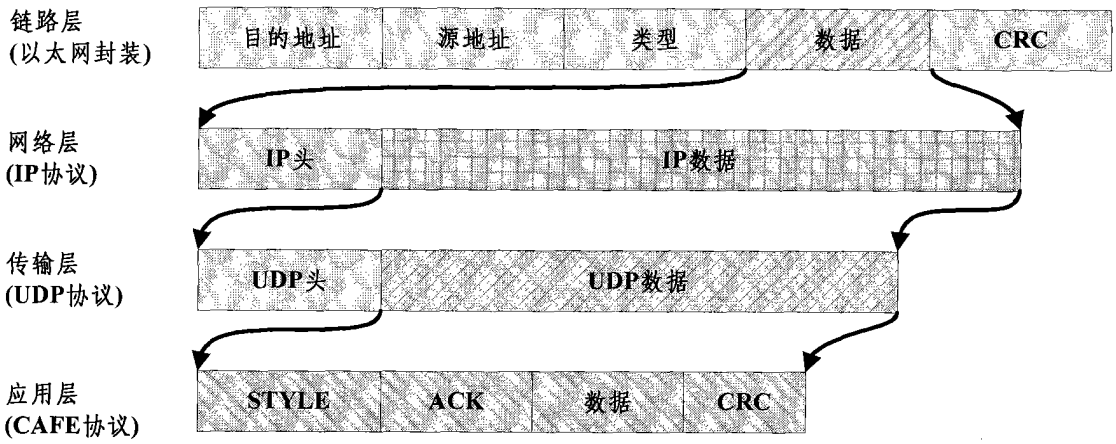

链路层
(以太网封装)
目的地址
源地址
类型
数据
CRC
网络层
(IP协议)
IP头
IP数据
传输层
(UDP协议)
UDP头
UDP数据
应用层
(CAFE协议)
STYLE
ACK
数据
CRC

图 4

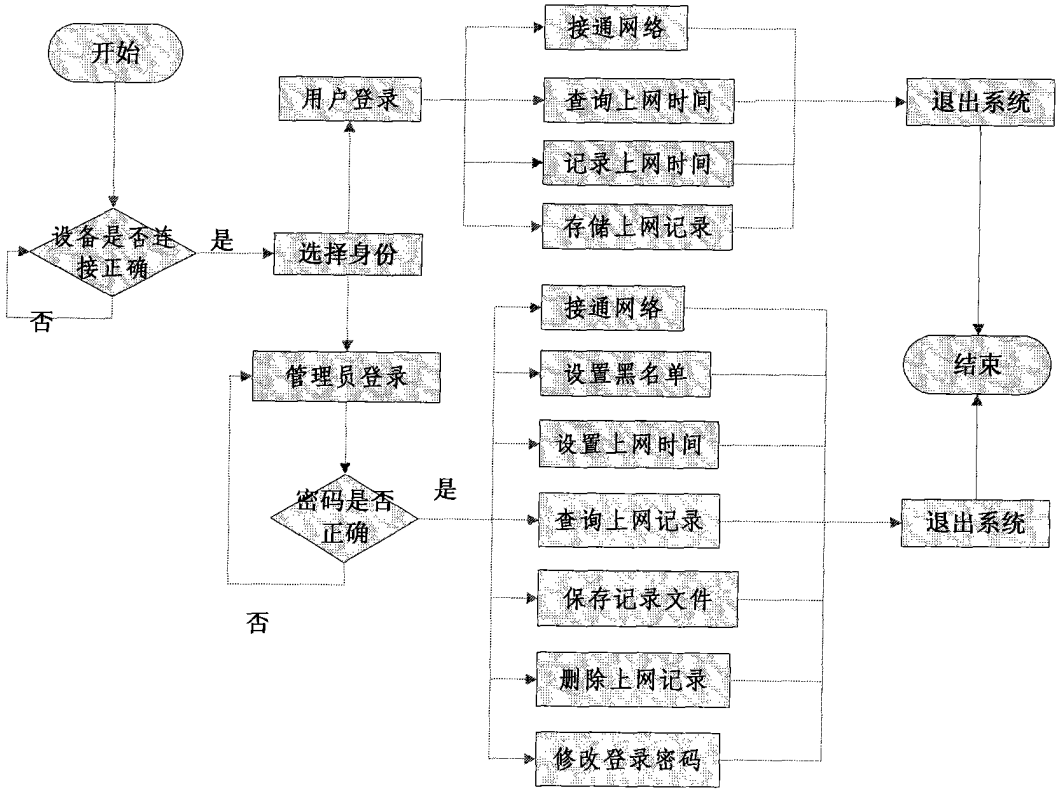

开始
设备是否连接正确
否
是
选择身份
用户登录
管理员登录
密码是否正确
否
是
接通网络
查询上网时间
记录上网时间
存储上网记录
退出系统
接通网络
设置黑名单
设置上网时间
查询上网记录
保存记录文件
删除上网记录
修改登录密码
退出系统
结束

图 5