(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 112866200 A
(43)申请公布日 2021.05.28

(21)申请号 202011633372.X

(22)申请日 2020.12.31

(71)申请人 深圳市东晟数据有限公司
地址 518000 广东省深圳市南山区粤海街道麻岭社区高新中二道2号深圳软件园1栋503

(72)发明人 卢佳晨

(74)专利代理机构 深圳市中科创为专利代理有限公司 44384
代理人 谭雪婷 梁炎芳

(51)Int.Cl.
*H04L 29/06*(2006.01)
*H04L 29/08*(2006.01)
*H04L 12/24*(2006.01)

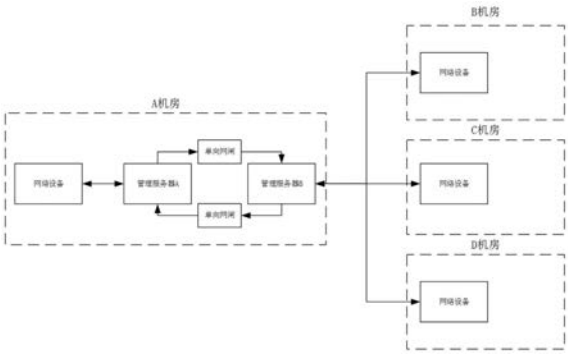
权利要求书2页 说明书5页 附图12页

(54)发明名称

一种复杂网络环境下的网络设备规则管理系统

(57)摘要

本发明公开了一种复杂网络环境下的网络设备规则管理系统，主机房还设置有管理服务器A、管理服务器B以及两个单向网闸，所述管理服务器A通过一个单向网闸与管理服务器B实现正向传输，所述管理服务器B通过另一个单向网闸与管理服务器A实现反向传输，所述管理服务器A与主机房的网络设备双向传输，所述管理服务器B与各分机房的网络设备双向传输，管理服务器A中部署RMS，管理服务器B部署RMS_GAP。本发明满足以下要求：使用特定单向网闸、使用特定的网络设备、不对设备进行二次开发以及各分机房互不联通，抵消新加入的单向网闸对现有业务的影响，保障业务正常运行。




CN 112866200 A

1.一种复杂网络环境下的网络设备规则管理系统,包括主机房和若干分机房,所述主机房分别与各分机房连接,所述主机房和各分机房分别设置有网络设备,其特征在于,所述主机房还设置有管理服务器A、管理服务器B以及两个单向网闸,所述管理服务器A通过一个单向网闸与管理服务器B实现正向传输,所述管理服务器B通过另一个单向网闸与管理服务器A实现反向传输,所述管理服务器A与主机房的网络设备双向传输,所述管理服务器B与各分机房的网络设备双向传输;

所述管理服务器A中部署RMS,负责接收Web系统的规则操作指令并转换为对主机房网络设备的设备操作、监听设备状态、监控规则状态;

所述管理服务器B部署RMS_GAP,负责接收RMS对各分机房的网络设备的操作指令并转换为对各分机房网络设备的设备操作。

2.根据权利要求1所述的复杂网络环境下的网络设备规则管理系统,其特征在于,所述RMS的结构包括TCP服务接口、RMS数据处理模块以及主机房数据库,所述Web系统通过JSON格式数据与TCP服务接口双向连接,所述TCP服务接口将解析后的数据传送至RMS数据处理模块,所述RMS数据处理模块将处理的数据返回至TCP服务接口;

所述RMS数据处理模块对主机房数据库中的信息进行数据库操作,数据库操作包括读取设备信息、读取规则信息、用户信息以及设备接口。

3.根据权利要求2所述的复杂网络环境下的网络设备规则管理系统,其特征在于,所述RMS数据处理模块包括主机房规则管理模块、主机房用户管理模块、主机房设备管理模块、主机房系统管理模块以及主机房文件监听模块,所述主机房规则管理模块用于处理规则下发操作并输出网闸传输文件,所述主机房文件监听模块用于监控网闸传输文件,所述主机房设备管理模块用于监控主机房的网络设备,所述主机房用户管理模块用于对用户鉴权校验,所述主机房系统管理模块用于日志记录和系统配置。

4.根据权利要求3所述的复杂网络环境下的网络设备规则管理系统,其特征在于,所述主机房规则管理模块处理规则下发操作时,对所有网络设备的信息进行判断,判断该网络设备是否为跨网闸设备:

若不为跨网闸设备,直接将请求转换为设备请求,发送至主机房网络设备;

若为跨网闸设备时,将请求转化为txt文本并使用UUID作为请求标识,将文本保存至网闸传输文件夹。

5.根据权利要求4所述的复杂网络环境下的网络设备规则管理系统,其特征在于,所述主机房文件监听模块使用Apache.commons.io下的File Alteration Listener Adaptor进行文件监听,对网闸传输过来的文件进行读取,根据请求标识回写结果。

6.根据权利要求5所述的复杂网络环境下的网络设备规则管理系统,其特征在于,所述主机房设备管理模块使用SNMP协议定时对所有的在线设备进行心跳请求,以确定设备是否在线,同时对已下线设备进行心跳请求,以确定设备是否已经正常启动,并对设备规则进行增量同步,其中规则下发过程由主机房规则管理模块进行操作。

7.根据权利要求5所述的复杂网络环境下的网络设备规则管理系统,其特征在于,所述主机房设备管理模块还使用SNMP Trap监听所有设备状态,并对错误信息进行分级处理和日志记录。

8.根据权利要求3所述的复杂网络环境下的网络设备规则管理系统,其特征在于,所述

RMS_GAP的结构包括RMS_GAP数据管理模块以及分机房数据库，RMS_GAP数据处理模块对分机房数据库中的信息进行数据库操作，数据库操作包括读取设备信息、读取规则信息以及设备接口。

9.根据权利要求8所述的复杂网络环境下的网络设备规则管理系统，其特征在于，RMS_GAP数据处理模块包括分机房规则管理模块、分机房设备管理模块、分机房系统管理模块以及分机房文件监听模块：

所述分机房文件监听模块用于监控网闸传输文件，所述分机房规则管理模块根据分机房文件监听模块读取的请求内容转化为对各分机房的RCP请求操作，所述分机房设备管理模块根据分机房文件监听模块读取的请求内容转化为对各分机房的snmp请求操作，所述分机房系统管理模块用于日志记录和系统配置。

# 一种复杂网络环境下的网络设备规则管理系统

## 技术领域

[0001] 本发明涉及网络安全和数据通信领域，尤其涉及的是一种复杂网络环境下的网络设备规则管理系统。

## 背景技术

[0002] 现有规则管理服务多为单机房部署或直连的多机房网络环境，如图1，为现有规则管理所适用的机房网络拓扑，在管理服务器收到规则操作消息后，直接将消息转换为设备操作消息转发至各网络设备即可。

[0003] 上述实现方案不适用于添加单向网闸后的网络环境，由于在添加单向网闸后，无法进行双向通信，故已有实现方案，无法对跨网闸设备进行规则管理，其中，单向网闸为一种采用无反馈的单向传输技术的装置，采用硬件隔离，从物理链路层、传输层保证数据的绝对单向流动。

[0004] 因此，现有技术存在缺陷，需要改进。

## 发明内容

[0005] 本发明所要解决的技术问题是：提供一种复杂网络环境下的网络设备规则管理系统，以解决上述技术问题。

[0006] 本发明的技术方案如下：一种复杂网络环境下的网络设备规则管理系统，包括主机房和若干分机房，所述主机房分别与各分机房连接，所述主机房和各分机房分别设置有网络设备，所述主机房还设置有管理服务器A、管理服务器B以及两个单向网闸，所述管理服务器A通过一个单向网闸与管理服务器B实现正向传输，所述管理服务器B通过另一个单向网闸与管理服务器A实现反向传输，所述管理服务器A与主机房的网络设备双向传输，所述管理服务器B与各分机房的网络设备双向传输；

[0007] 所述管理服务器A中部署RMS，负责接收Web系统的规则操作指令并转换为对主机房网络设备的设备操作、监听设备状态、监控规则状态；

[0008] 所述管理服务器B部署RMS_GAP，负责接收RMS对各分机房的网络设备的操作指令并转换为对各分机房网络设备的设备操作。

[0009] 采用上述技术方案，所述的复杂网络环境下的网络设备规则管理系统，所述RMS的结构包括TCP服务接口、RMS数据处理模块以及主机房数据库，所述Web系统通过JSON格式数据与TCP服务接口双向连接，所述TCP服务接口将解析后的数据传送至RMS数据处理模块，所述RMS数据处理模块将处理的数据返回至TCP服务接口；

[0010] 所述RMS数据处理模块对主机房数据库中的信息进行数据库操作，数据库操作包括读取设备信息和读取规则信息。

[0011] 采用上述技术方案，所述的复杂网络环境下的网络设备规则管理系统，所述RMS数据处理模块包括主机房规则管理模块、主机房用户管理模块、主机房设备管理模块、主机房系统管理模块以及主机房文件监听模块，所述主机房规则管理模块用于处理规则下发操作

并输出网闸传输文件，所述主机房文件监听模块用于监控网闸传输文件，所述主机房设备管理模块用于监控主机房的网络设备，所述主机房用户管理模块用于对用户鉴权校验，所述主机房系统管理模块用于日志记录和系统配置。

[0012] 采用上述技术方案，所述的复杂网络环境下的网络设备规则管理系统，所述主机房规则管理模块处理规则下发操作时，对所有网络设备的信息进行判断，判断该网络设备是否为跨网闸设备：

[0013] 若不为跨网闸设备，直接将请求转换为设备请求，发送至主机房网络设备；

[0014] 若为跨网闸设备时，将请求转化为txt文本并使用UUID作为请求标识，将文本保存至网闸传输文件夹。

[0015] 采用上述技术方案，所述的复杂网络环境下的网络设备规则管理系统，所述主机房文件监听模块使用Apache.commons.io下的File Alteration Listener Adaptor进行文件监听，对网闸传输过来的文件进行读取，根据请求标识回写结果。

[0016] 采用上述技术方案，所述的复杂网络环境下的网络设备规则管理系统，所述主机房设备管理模块使用SNMP协议定时对所有的在线设备进行心跳请求，以确定设备是否在线，同时对已下线设备进行心跳请求，以确定设备是否已经正常启动，并对设备规则进行增量同步，其中规则下发过程由主机房规则管理模块进行操作启动。

[0017] 采用上述技术方案，所述的复杂网络环境下的网络设备规则管理系统，所述主机房设备管理模块还使用SNMP Trap监听所有设备状态，并对错误信息进行分级处理和日志记录。

[0018] 采用上述技术方案，所述的复杂网络环境下的网络设备规则管理系统，所述RMS_GAP的结构包括RMS_GAP数据管理模块以及分机房数据库，RMS_GAP数据处理模块对分机房数据库中的信息进行数据库操作，数据库操作包括读取设备信息、读取规则信息以及设备接口。

[0019] 采用上述技术方案，所述的复杂网络环境下的网络设备规则管理系统，RMS_GAP数据处理模块包括分机房规则管理模块、分机房设备管理模块、分机房系统管理模块以及分机房文件监听模块：

[0020] 所述分机房文件监听模块用于监控网闸传输文件，所述分机房规则管理模块根据分机房文件监听模块读取的请求内容转化为对各分机房的RCP请求操作，所述分机房设备管理模块根据分机房文件监听模块读取的请求内容转化为对各分机房的snmp请求操作，所述分机房系统管理模块用于日志记录和系统配置。

[0021] 采用上述各个技术方案，本发明满足以下要求：使用特定单向网闸、使用特定的网络设备、不对设备进行二次开发以及各分机房互不联通，抵消新加入的单向网闸对现有业务的影响，保障业务正常运行。

## 附图说明

[0022] 图1为现有网络拓扑结构示意图；

[0023] 图2为本发明的机房网络拓扑结构示意图；

[0024] 图3为本发明的RMS结构示意图；

[0025] 图4为本发明的RMS规则管理模块流程示意图；

[0026] 图5为本发明的RMS文件监听模块流程示意图；

[0027] 图6为本发明的RMS TCP服务接口流程示意图；

[0028] 图7为本发明的RMS设备管理模块的设备心跳流程示意图；

[0029] 图8为本发明的RMS设备心跳具体过程示意图；

[0030] 图9为本发明的RMS设备管理模块的SNMP Trap监听流程示意图；

[0031] 图10为本发明的RMS_GAP结构示意图；

[0032] 图11为本发明的RMS_GAP规则管理模块示意图；

[0033] 图12为本发明的RMS_GAP设备管理模块示意图；

[0034] 图13为本发明的RMS_GAP文件监听模块示意图。

## 具体实施方式

[0035] 以下结合附图和具体实施例，对本发明进行详细说明。

[0036] 如图2，本实施例提供了一种复杂网络环境下的网络设备规则管理系统，包括主机房和若干分机房，所述主机房分别与各分机房连接，所述主机房和各分机房分别设置有网络设备。为了表述方便，以A机房表示主机房，以B、C、D机房表示各分机房。所述主机房还设置有管理服务器A、管理服务器B以及两个单向网闸，所述管理服务器A通过一个单向网闸与管理服务器B实现正向传输，所述管理服务器B通过另一个单向网闸与管理服务器A实现反向传输，所述管理服务器A与主机房的网络设备双向传输，所述管理服务器B与各分机房的网络设备双向传输。

[0037] 如图2，管理服务器A中部署RMS，负责接收Web系统的规则操作指令并转换为对主机房网络设备的设备操作、监听设备状态、监控规则状态。管理服务器B部署RMS_GAP，负责接收RMS对各分机房的网络设备的操作指令并转换为对各分机房网络设备的设备操作。

[0038] 其中，RMS中的所有设备操作都是针对A机房的网络设备，RMS_GAP中所有设备操作都是针对B、C、D机房的网络设备。

[0039] 如图3，所述RMS的结构包括TCP服务接口、RMS数据处理模块以及数据库，所述Web系统通过JSON格式数据与TCP服务接口双向连接，所述TCP服务接口将解析后的数据传送至RMS数据处理模块，所述RMS数据处理模块将处理的数据返回至TCP服务接口。

[0040] 所述RMS数据处理模块对数据库中的信息进行数据库操作，数据库操作包括但不限于读取设备信息、读取规则信息、用户信息以及设备接口等。RMS数据处理模块通过RCP，SNMP协议与A机房的网络设备进行传输。RCP(Rule Configuration Protocol)是专门为安全项目开发的私有的应用层协议，它主要完成客户主机到网络设备之间规则的传递；SNMP(Simple Network Management Protocol)是目前TCP/IP网络应用最为广泛的网络管理协议，它主要完成监视网络状态、修改网络设备配置、接受网络事件警告、设备心跳检测等。

[0041] 如图3，RMS数据处理模块包括主机房规则管理模块、主机房用户管理模块、主机房设备管理模块、主机房系统管理模块以及文件监听模块。主机房规则管理模块用于处理规则下发操作并输出网闸传输文件，主机房文件监听模块用于监控网闸传输文件，主机房设备管理模块用于监控主机房的网络设备，用户管理模块用于对用户鉴权校验，主机房系统管理模块用于日志记录和系统配置。

[0042] RMS数据处理模块中的各模块没有必然的一一对应关系，根据需求进行互相调用。

例如,主机房设备管理模块要监控A机房的网络设备时,则调用主机房系统管理模块中的日志。主机房设备管理模块监控A机房的网络设备时,调用主机房监听文件模块中的结果。

[0043] 如规则操作时,先调用主机房用户管理模块进行认证,在调用主机房规则管理进行解析,调用主机房设备管理模块查询设备信息,调用主机房文件监听模块,当有日志操作时,再调用主机房系统管理模块中的日志。

[0044] 需要说明的是,主机房用户管理模块则不会被主动调用,用户信息在部署时已经固化在程序中,仅进行鉴权操作。

[0045] 主机房规则管理模块处理规则下发操作时,对主机房和分机房的所有网络设备的信息进行判断,判断该网络设备是否为跨网闸设备:

[0046] 若不为跨网闸设备,直接将请求转换为设备请求,发送至主机房网络设备;

[0047] 若为跨网闸设备时,将请求转化为txt文本并使用UUID作为请求标识,将文本保存至网闸传输文件夹。

[0048] 主机房规则管理模块处理规则下发操作的具体流程如图4。

[0049] 主机房文件监听模块使用Apache.commons.io下的File Alteration Listener Adaptor进行文件监听,对网闸传输过来的文件进行读取,根据请求标识回写结果。

[0050] 主机房文件监听模块的具体流程如图5。

[0051] 如图6,为TCP服务接口的具体流程示意图,与Web系统交互接口,使用JSON格式数据进行交互,其中业务处理过程调用规则管理模块。

[0052] 主机房设备管理模块使用SNMP协议定时对所有的在线设备进行心跳请求,以确定设备是否在线,同时对已下线设备进行心跳请求,以确定设备是否已经正常启动,并对设备规则进行增量同步,其中规则下发过程由规则管理模块进行操作启动。

[0053] 如图7为主机房设备管理模块监控设备心跳的具体流程示意图,图8则为心跳的具体流程示意图。

[0054] 图7中,设备重启操作为所有网络设备(包含主机房和各分机房)重启,系统重启操作为规则管理系统(RMS)重启。

[0055] 如图9,为RMS设备管理模块的SNMP Trap监听流程示意图,使用SNMP Trap监听所有设备状态,并对错误信息进行分级处理,使用邮箱等手段进行通知,并日志记录。

[0056] 如图10,所述RMS_GAP的结构包括RMS_GAP数据管理模块以及分机房数据库,RMS_GAP数据处理模块对分机房数据库中的信息进行数据库操作,数据库操作包括读取设备信息、读取规则信息以及设备接口。RMS_GAP数据处理模块包括分机房规则管理模块、分机房设备管理模块、分机房系统管理模块以及分机房文件监听模块:

[0057] 如图10,分机房文件监听模块用于监控网闸传输文件,如图11,分机房规则管理模块根据分机房文件监听模块读取的请求内容转化为对各分机房的RCP请求操作,如图12,分机房设备管理模块根据分机房文件监听模块读取的请求内容转化为对各分机房的snmp请求操作,分机房系统管理模块用于日志记录和系统配置。

[0058] 如图13,分机房文件监听模块监听网闸传输文件,根据文件内容调用不同的功能模块进行业务操作。

[0059] 采用上述各个技术方案,本发明满足以下要求:使用特定单向网闸、使用特定的网络设备、不对设备进行二次开发以及各分机房互不联通,抵消新加入的单向网闸对现有业

务的影响，保障业务正常运行。

[0060] 以上仅为本发明的较佳实施例而已，并不用于限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

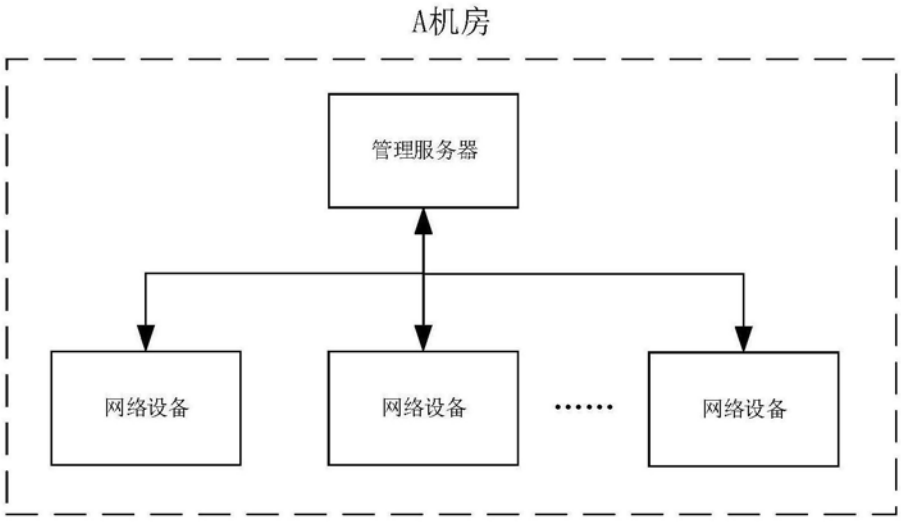

A机房
管理服务器
网络设备
网络设备
网络设备

图1

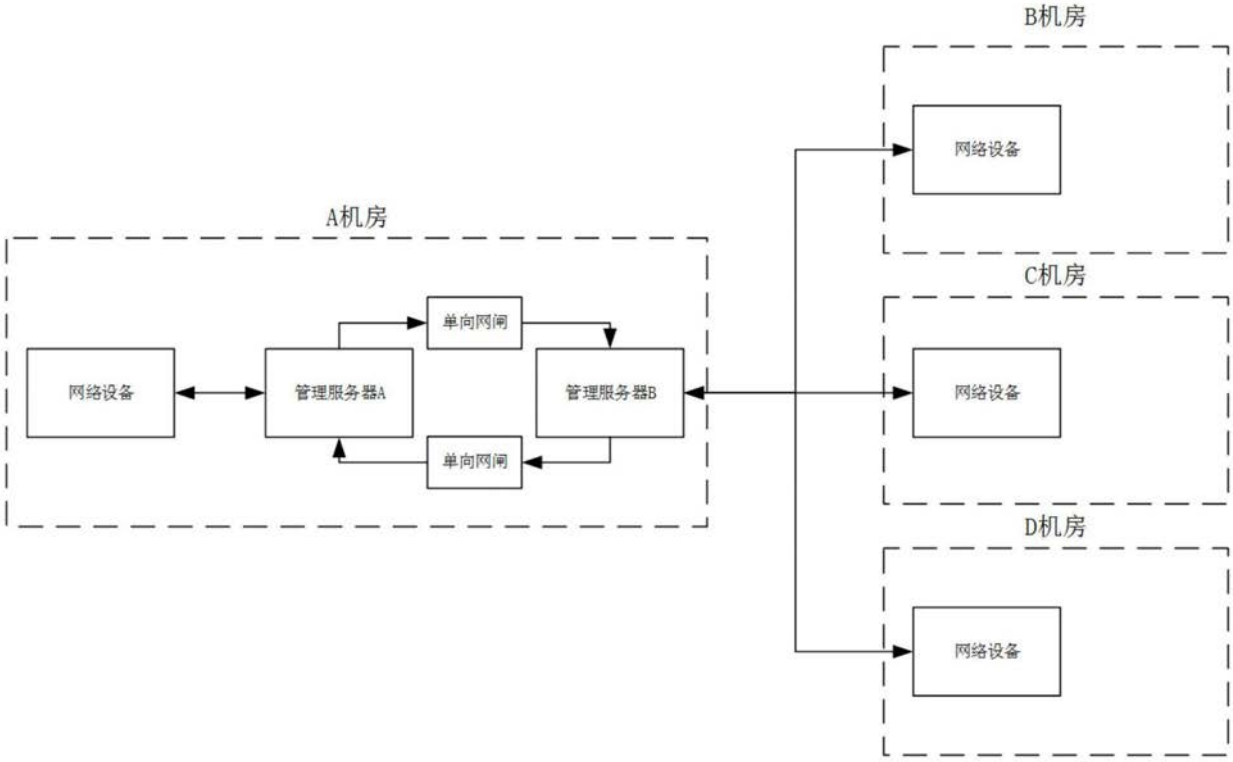

B机房
网络设备
A机房
C机房
单向网闸
网络设备
管理服务器A
管理服务器B
网络设备
单向网闸
D机房
网络设备

图2

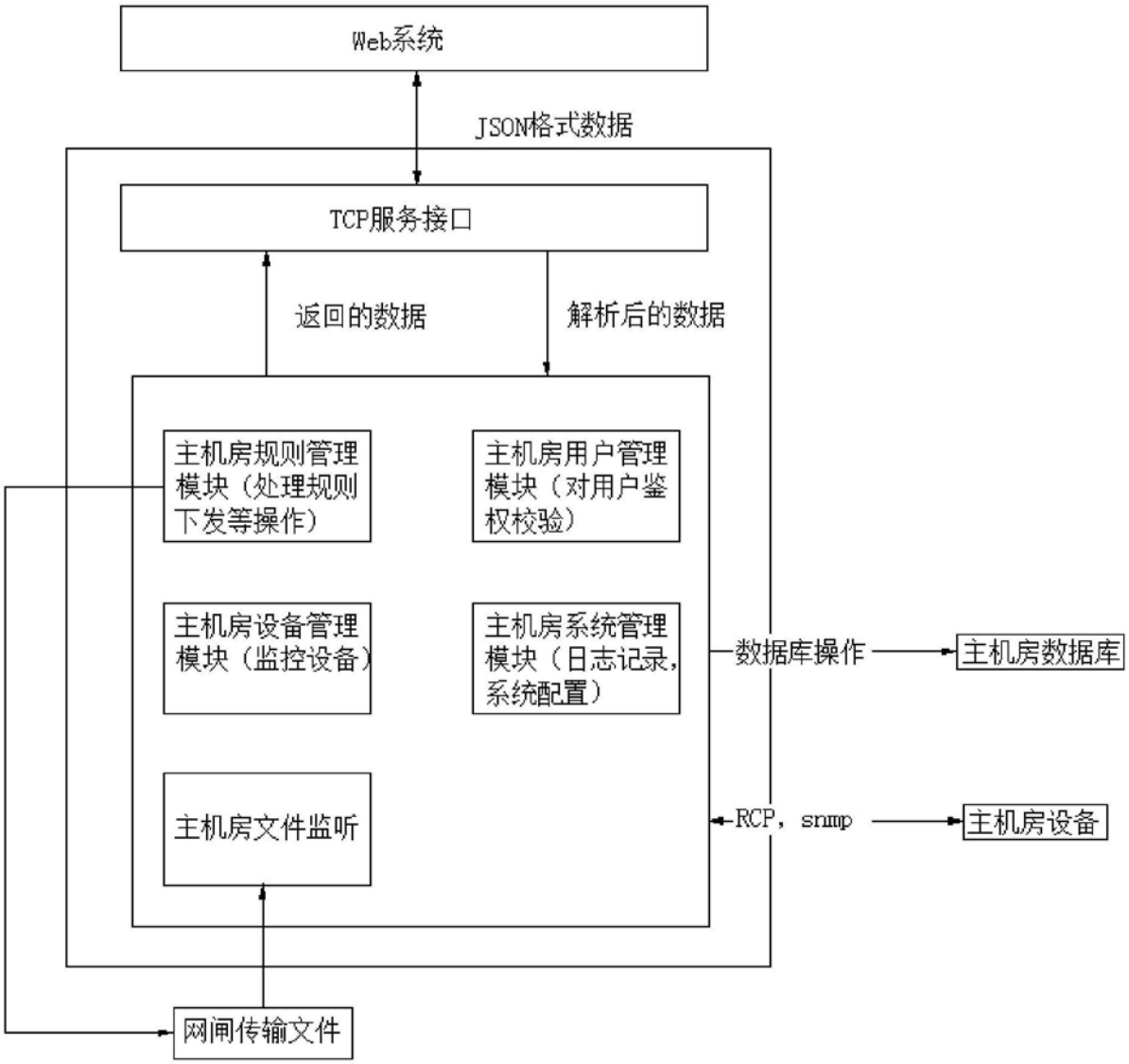

Web系统
JSON格式数据
TCP服务接口
返回的数据
解析后的数据
主机房规则管理模块（处理规则下发等操作）
主机房用户管理模块（对用户鉴权校验）
主机房设备管理模块（监控设备）
主机房系统管理模块（日志记录，系统配置）
主机房文件监听
数据库操作
主机房数据库
RCP，snmp
主机房设备
网闸传输文件

图3

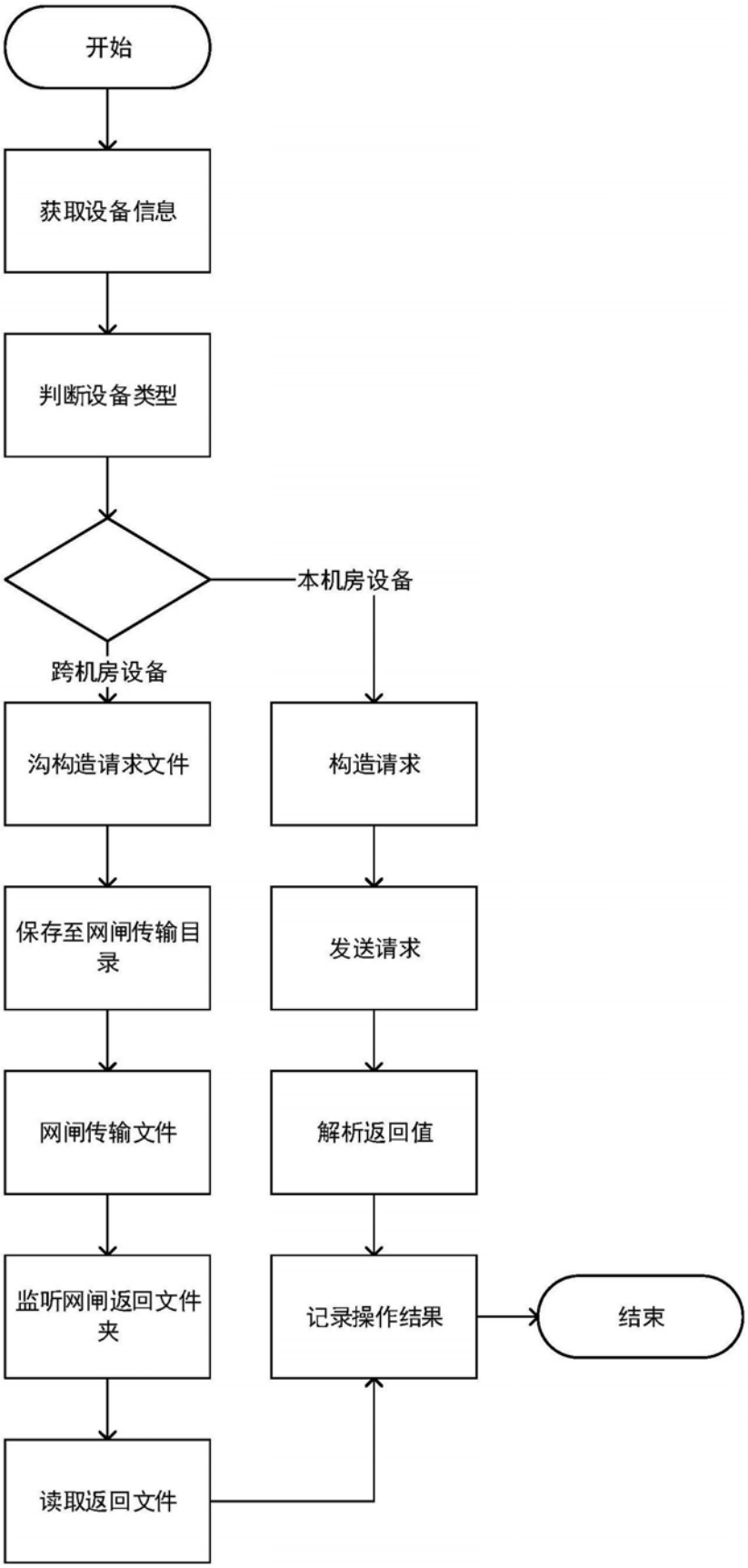

开始
获取设备信息
判断设备类型
本机房设备
跨机房设备
沟构造请求文件
构造请求
保存至网闸传输目录
发送请求
网闸传输文件
解析返回值
监听网闸返回文件夹
记录操作结果
结束
读取返回文件

图4

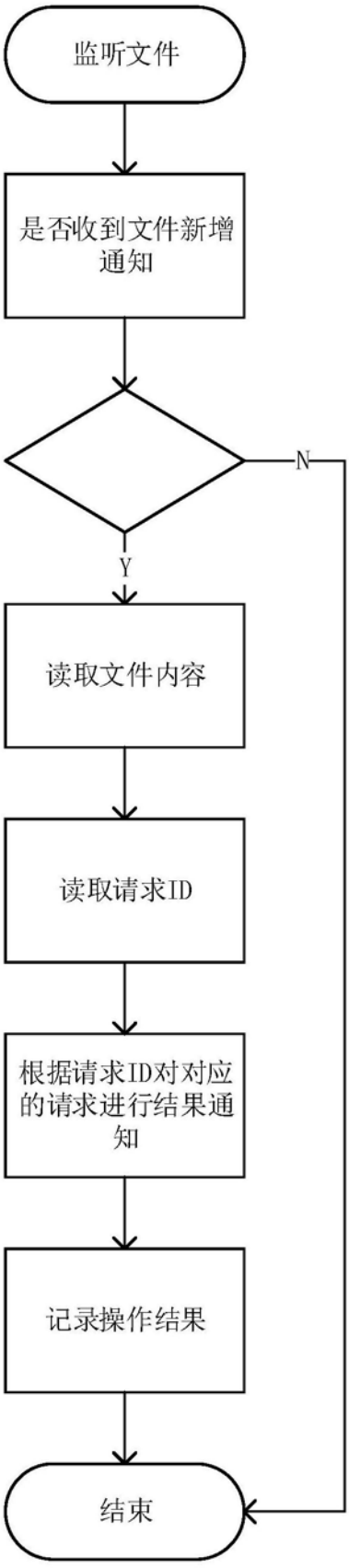

监听文件
是否收到文件新增通知
N
Y
读取文件内容
读取请求ID
根据请求ID对对应的请求进行结果通知
记录操作结果
结束

图5

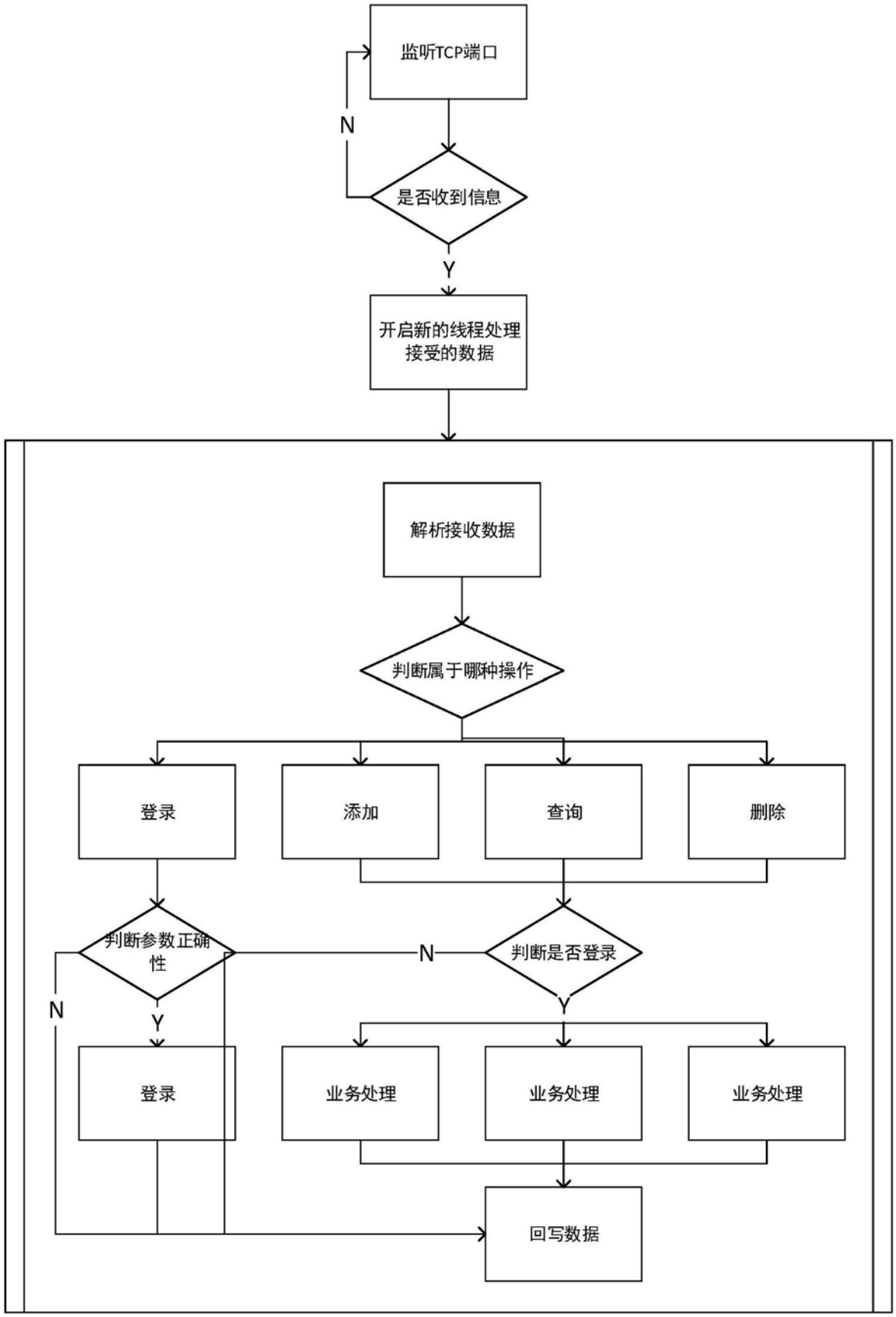

监听TCP端口
N
是否收到信息
Y
开启新的线程处理接受的数据
解析接收数据
判断属于哪种操作
登录
添加
查询
删除
判断参数正确性
N
判断是否登录
N
Y
Y
登录
业务处理
业务处理
业务处理
回写数据

图6

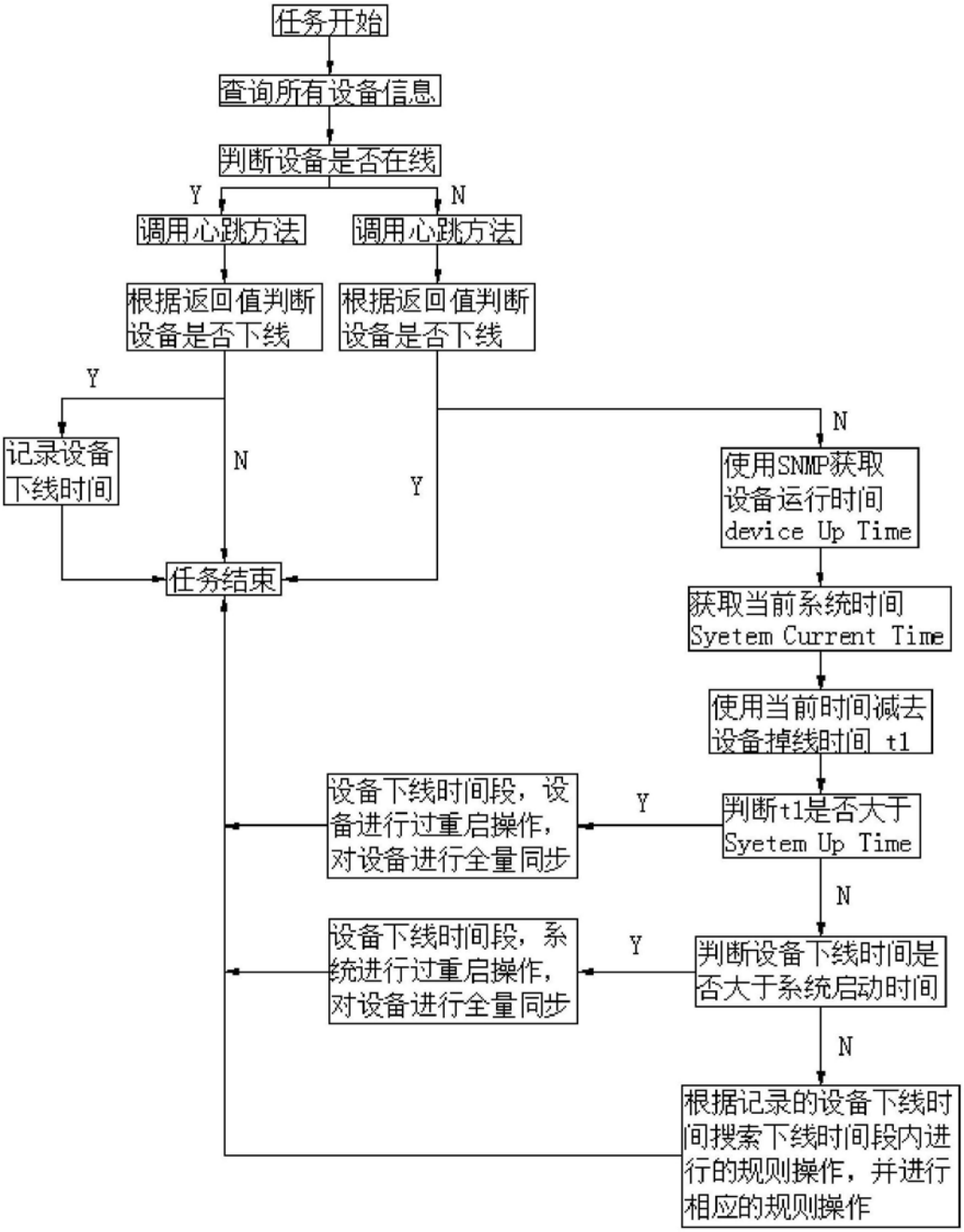

任务开始
查询所有设备信息
判断设备是否在线
Y
N
调用心跳方法
调用心跳方法
根据返回值判断设备是否下线
根据返回值判断设备是否下线
Y
N
Y
N
记录设备下线时间
使用SNMP获取设备运行时间 device Up Time
任务结束
获取当前系统时间 Syetem Current Time
使用当前时间减去设备掉线时间 t1
设备下线时间段，设备进行过重启操作，对设备进行全量同步
Y
判断t1是否大于 Syetem Up Time
N
设备下线时间段，系统进行过重启操作，对设备进行全量同步
Y
判断设备下线时间是否大于系统启动时间
N
根据记录的设备下线时间搜索下线时间段内进行的规则操作，并进行相应的规则操作

图7

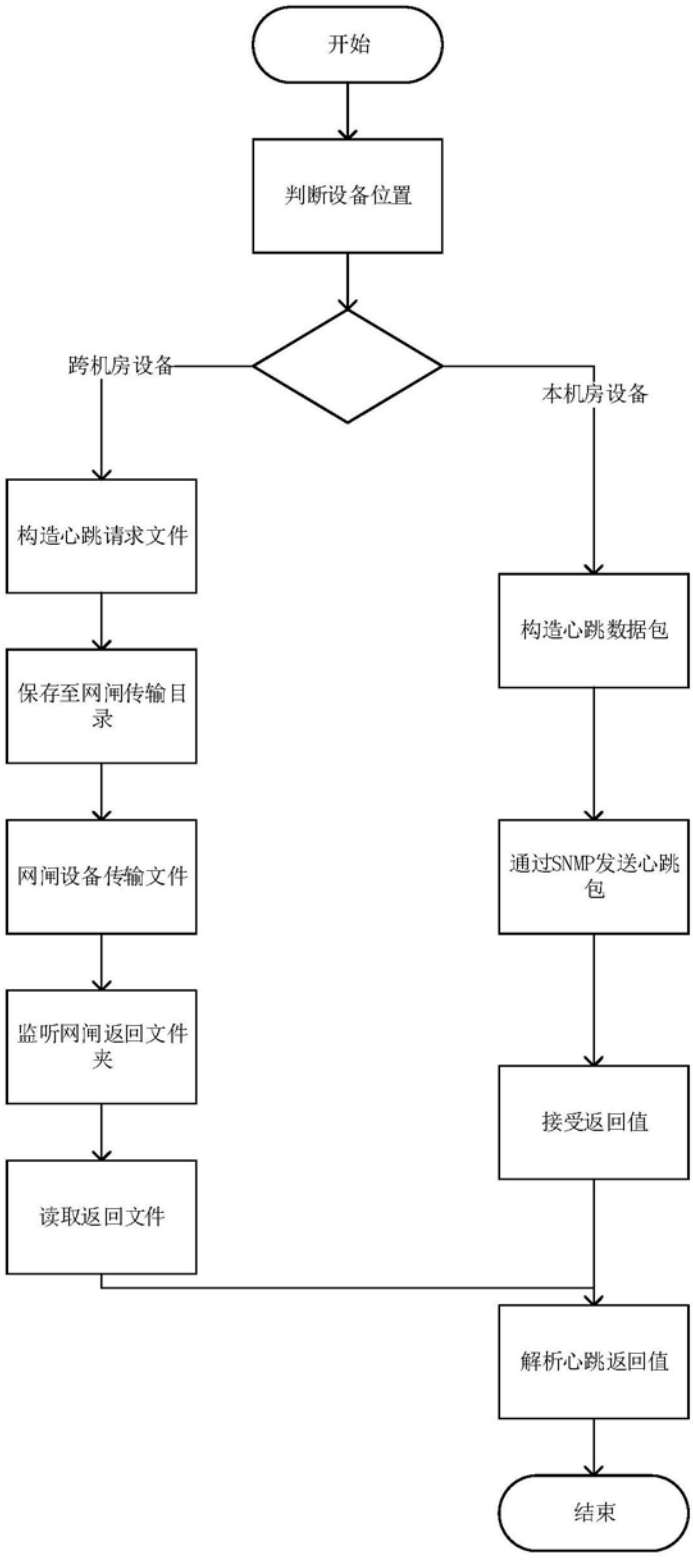

开始
判断设备位置
跨机房设备
本机房设备
构造心跳请求文件
保存至网闸传输目录
网闸设备传输文件
监听网闸返回文件夹
读取返回文件
构造心跳数据包
通过SNMP发送心跳包
接受返回值
解析心跳返回值
结束

图8

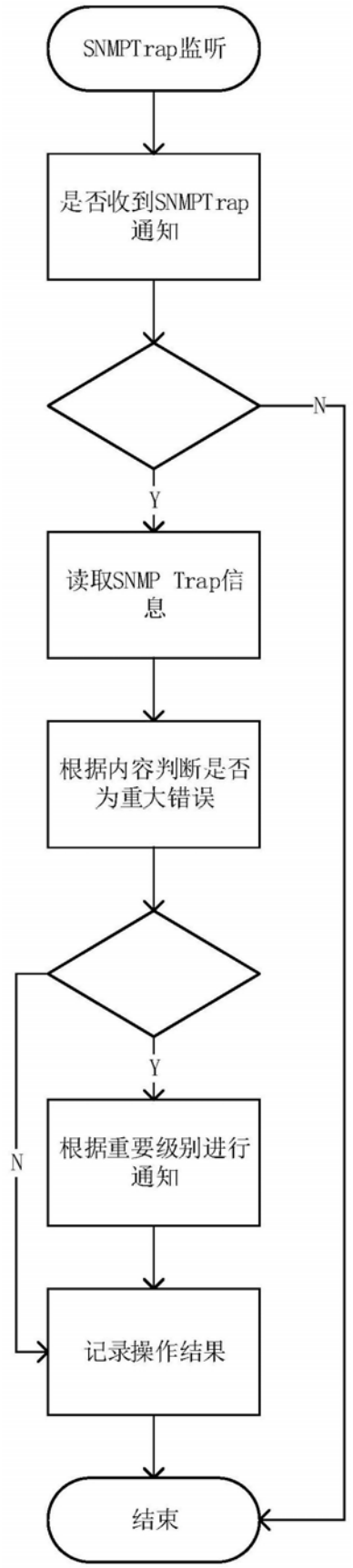

SNMPTrap监听
是否收到SNMPTrap通知
N
Y
读取SNMP Trap信息
根据内容判断是否为重大错误
Y
N
根据重要级别进行通知
记录操作结果
结束

图9

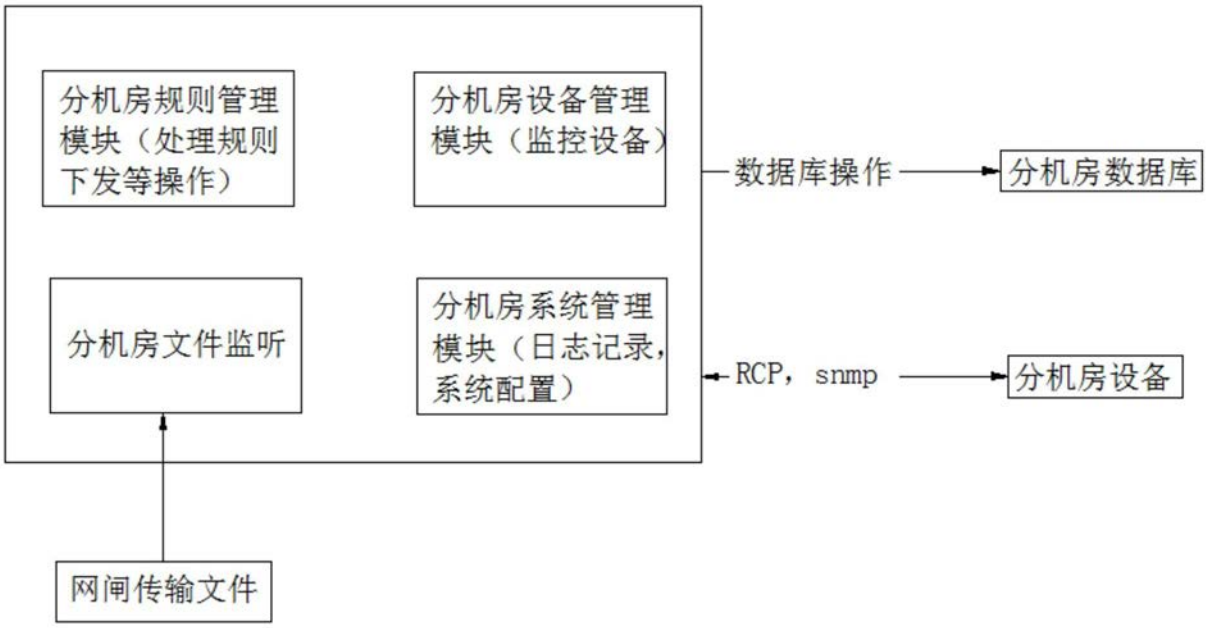

分机房规则管理模块（处理规则下发等操作）
分机房设备管理模块（监控设备）
数据库操作
分机房数据库
分机房文件监听
分机房系统管理模块（日志记录，系统配置）
RCP，snmp
分机房设备
网闸传输文件

图10

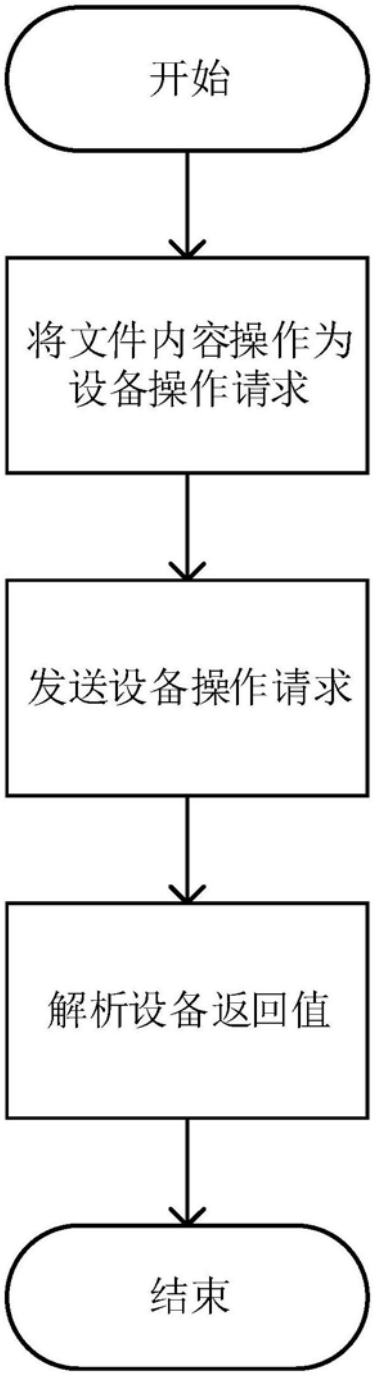



图11

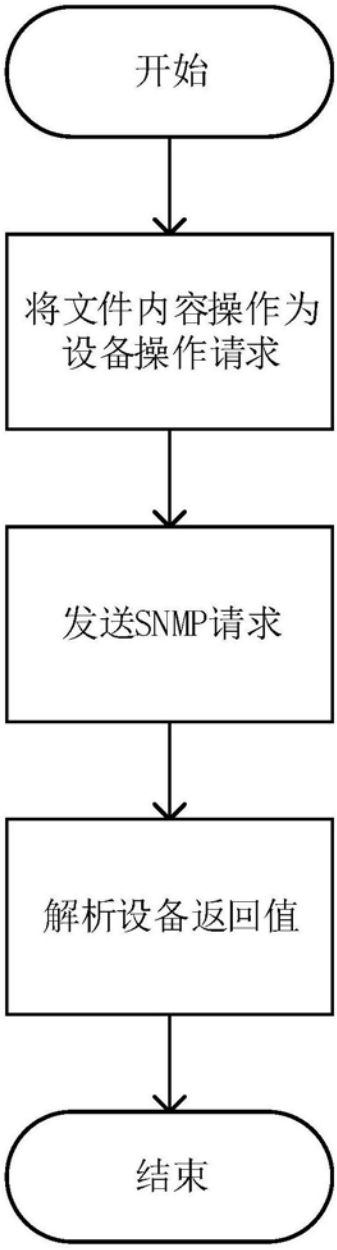



图12

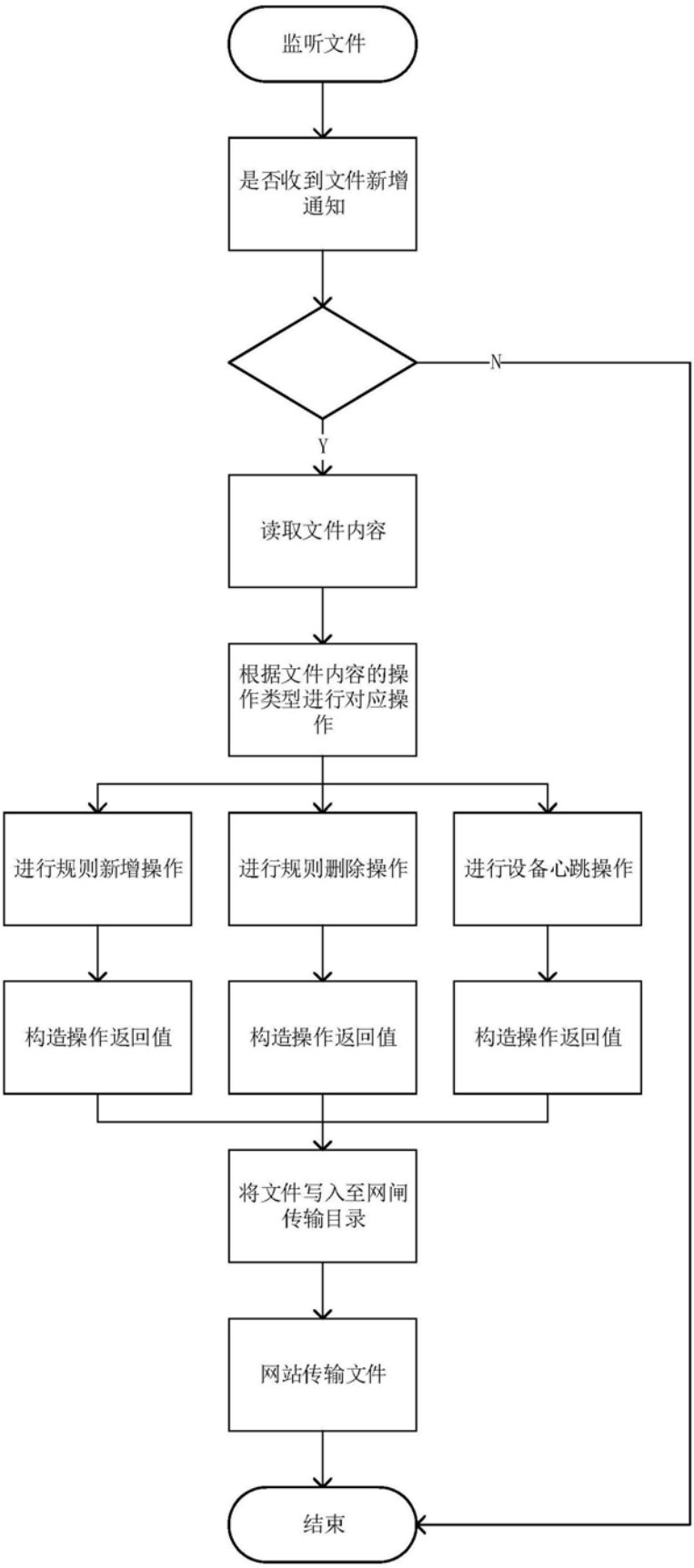

监听文件
是否收到文件新增通知
N
Y
读取文件内容
根据文件内容的操作类型进行对应操作
进行规则新增操作
进行规则删除操作
进行设备心跳操作
构造操作返回值
构造操作返回值
构造操作返回值
将文件写入至网闸传输目录
网站传输文件
结束

图13