(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101312405 B
(45)授权公告日 2011.06.08

(21)申请号 200710107668.6

(22)申请日 2007.05.24

(73)专利权人 杭州华三通信技术有限公司
地址 310053 浙江省杭州市高新技术产业开发区之江科技工业园六和路 310 号

(72)发明人 黄小东

(74)专利代理机构 北京鑫媛睿博知识产权代理有限公司 11297
代理人 龚家骅

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

(56)对比文件
KR 2003-0018833 A,2003.03.06,

审查员 张劲松

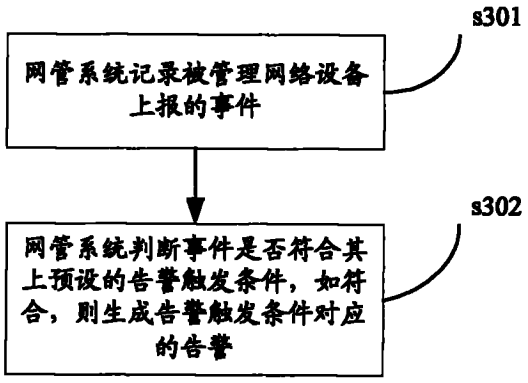
权利要求书 1 页 说明书 5 页 附图 3 页

(54)发明名称

一种告警处理方法及网管系统

(57)摘要

本发明提供了一种告警处理方法,应用于网络管理系统对被管理网络设备的告警分析,所述方法包括以下步骤:网管系统记录被管理网络设备上报的事件;所述网管系统判断所述事件是否符合其上预设的告警触发条件,如符合,则生成所述告警触发条件对应的告警。本发明的实施例中,通过预先设置告警触发条件,实现灵活告警过滤分析,满足不同用户的各种需求;另外,由于所有事件都保存在网管系统中,可以通过告警查看关联的事件,也可以事后追查具体的事件上报情况;再有,由于通过定义规则实现告警过滤的功能,因此易于扩展。




CN 101312405 B

1. 一种告警处理方法，应用于网管系统对被管理网络设备的告警分析，其特征在于，所述方法包括以下步骤：

网管系统记录被管理网络设备上报的事件；

所述网管系统判断所述事件是否符合其上预设的告警触发条件，如符合，则生成所述告警触发条件对应的告警；其中，

所述网管系统记录被管理网络设备上报的事件具体包括：所述网管系统接收来自被管理网络设备上报的事件；所述网管系统将所述上报的事件解析，并存入事件库。

2. 如权利要求 1 所述告警处理方法，其特征在于，所述生成告警后还包括：所述网管系统保存所述对应的告警。

3. 如权利要求 2 所述告警处理方法，其特征在于，所述预设的告警触发条件是可根据用户需求动态修改的。

4. 如权利要求 1 所述告警处理方法，其特征在于，所述告警触发条件包括：重复事件触发、关键字触发、闪断事件触发、未知事件触发、未管理设备触发、事件源触发、事件类型触发和时间范围触发中的任意一种触发或者大于等于两种触发的组合。

5. 如权利要求 1 至 4 中任一项所述告警处理方法，其特征在于，所述上报的事件包括：简单网络管理协议陷阱 SNMP Trap 事件或系统日志 Syslog 事件。

6. 一种网管系统，应用于具有告警分析功能的通信网络，其特征在于，包括：

上报事件获取单元，用于从被管理网络设备获取并记录上报事件；具体用于接收来自被管理网络设备上报的事件；将所述上报的事件解析并存入事件库；

告警生成单元，用于判断所述上报事件是否符合其上预设的告警触发条件，当符合时，生成所述告警触发条件对应的告警。

7. 如权利要求 6 所述网管系统，其特征在于，还包括告警存储单元，用于存储所述告警。

8. 如权利要求 6 所述网管系统，其特征在于，还包括告警触发条件更新单元，用于根据用户需求动态修改所述预设的告警触发条件。

9. 如权利要求 6 至 8 中任一项所述网管系统，其特征在于，所述告警触发条件包括：重复事件触发、关键字触发、闪断事件触发、未知事件触发、未管理设备触发、事件源触发、事件类型触发和时间范围触发中的任意一种触发或者大于等于两种触发的组合。

# 一种告警处理方法及网管系统

## 技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种告警处理方法及网管系统。

## 背景技术

[0002] 网络管理系统（简称网管系统）的一个最重要功能是通过告警来反映被管理网络设备的运行状态是否出现故障，并及时通知管理员。网管系统的告警信息采集包括：对被管理网络设备进行轮询，例如 ping 被管理的网络设备，判断该网络设备的存活状况或丢包率，进而确定该网络设备是否存在告警；或网管系统接收被管理网络设备发过来的 Syslog（系统日志），并通过相应的规则库（例如正则表达式等）匹配判断是否存在告警；或网管系统通过在固定端口接收被管理设备的 SNMP(Simple Network Management Protocol，简单网络管理协议）Trap（陷阱）告警报文确定产生告警；或通过远程调用等方式获知网络设备的运行情况。

[0003] 如图 1 所示，网管系统解析被管理网络设备发来的 Trap 告警或 Syslog 事件并保存，以供管理员了解网络设备的运行情况；另外，可以通过轮询发现被管理网络设备出现故障，例如轮询没有响应则网管系统自身产生一条告警信息。通过上述几种告警方式在网管系统将产生大量的告警信息，虽然某些告警可以通过自动恢复的方式来减少管理员需关注告警的数量，但仍然存在大量意义不大的告警信息充斥在网管系统中，需要管理员来人工判断，从而降低了管理员对有用告警的关注。因此网管系统除了不漏报告警的问题，同时还需要解决不要错报告警的问题。如果能找到一种简单有效的告警过滤分析的方法，就可以减少无效告警的数量，提高网管系统告警的可用性。

[0004] 目前已有网管系统实现了简单的告警过滤功能，该网管系统通过定义需过滤设备、告警类型和告警变量的方式来决定告警是否接收。具体工作流程如图 2 所示，包括：

[0005] 步骤 s201，网管系统接收来自被管理网络设备的告警信息，并将该告警信息解析。

[0006] 步骤 s202，网管系统判断发送该告警信息的网络设备、告警类型、参数是否与预设的过滤告警匹配，如果匹配，则说明此告警为用户预先设定需要过滤掉的告警，转步骤 s204；如果不匹配，则说明此告警不是用户想要过滤掉的告警，转步骤 s203。

[0007] 步骤 s203，网管系统保存该告警信息。

[0008] 步骤 s204，网管系统丢弃该告警信息。

[0009] 但是上述告警过滤方法存在以下较严重问题：非常不灵活，比如某些告警产生一次可能不需要关注，但如果频繁产生则需要关注，因此该方案无法满足各种用户告警过滤的需求。另外，被过滤的告警没有任何记录，不能进行追查审计，极有可能导致告警漏报。

[0010] 为了解决上述方案中告警过滤方式的缺陷，现有技术中还提出了使用告警关联分析的方式来减少告警的数量的方法，通过分析告警之间的关联性，只将重要的告警呈现给管理员，而和这些重要告警相关的次要告警则会被自动屏蔽掉，但仍然会记录，如果用户需要查看可以查询到这些被关联屏蔽掉的告警。

[0011] 然而，这种告警关联技术算法实现非常复杂，消耗大量开发成本，且不易进行扩

展，增加新告警功能。

[0012] 发明内容

[0013] 本发明实施例提供一种告警处理方法及网管系统，以解决现有技术中告警分析实现复杂，不易扩展的缺陷。

[0014] 本发明提供了一种告警处理方法，应用于网管系统对被管理网络设备的告警分析，所述方法包括以下步骤：

[0015] 网管系统记录被管理网络设备上报的事件；

[0016] 所述网管系统判断所述事件是否符合其上预设的告警触发条件，如符合，则生成所述告警触发条件对应的告警；其中，

[0017] 所述网管系统记录被管理网络设备上报的事件具体包括：所述网管系统接收来自被管理网络设备上报的事件；所述网管系统将所述上报的事件解析，并存入事件库。

[0018] 所述生成告警后还包括：所述网管系统保存所述对应的告警。

[0019] 所述预设的告警触发条件是可根据用户需求动态修改的。

[0020] 所述告警触发条件包括：重复事件触发、关键字触发、闪断事件触发、未知事件触发、未管理设备触发、事件源触发、事件类型触发和时间范围触发中的任意一种触发或者大于等于两种触发的组合。

[0021] 所述上报的事件包括：简单网络管理协议陷阱 SNMP Trap 事件或系统日志 Syslog 事件。

[0022] 本发明还提供了一种网管系统，应用于具有告警分析功能的通信网络，包括：

[0023] 上报事件获取单元，用于从被管理网络设备获取并记录上报事件；具体用于接收来自被管理网络设备上报的事件；将所述上报的事件解析并存入事件库；

[0024] 告警生成单元，用于判断所述上报事件是否符合其上预设的告警触发条件，当符合时，生成所述告警触发条件对应的告警。

[0025] 还包括告警存储单元，用于存储所述告警。

[0026] 还包括告警触发条件更新单元，用于根据用户需求动态修改所述预设的告警触发条件。

[0027] 所述告警触发条件包括：重复事件触发、关键字触发、闪断事件触发、未知事件触发、未管理设备触发、事件源触发、事件类型触发和时间范围触发中的任意一种触发或者大于等于两种触发的组合。

[0028] 与现有技术相比，本发明实施例具有以下优点：

[0029] 本发明的实施例中，通过预先设置告警触发条件，实现灵活告警过滤分，满足不同用户的各种需求；另外，由于所有事件都保存在网管系统中，可以通过告警查看关联的事件，也可以事后追查具体的事件上报情况；再有，由于通过定义规则实现告警过滤的功能，因此易于扩展，如果现有的告警触发条件不能满足用户需求，可以很容易地根据用户要求重新设计新的告警触发条件。

## 附图说明

[0030] 图 1 是现有技术中网管系统告警机制的示意图；

[0031] 图 2 是现有技术中告警过滤处理流程图；

[0032] 图 3 是本发明实施例中一种告警处理方法流程图；

[0033] 图 4 是本发明实施例中另一种告警处理方法流程图；

[0034] 图 5 是本发明实施例中又一种告警处理方法流程图；

[0035] 图 6 是本发明实施例中一种告警处理系统结构图。

## 具体实施方式

[0036] 下面结合附图和实施例，对本发明的具体实施方式作进一步详细描述：

[0037] 如图 3 所示，为本发明实施例一种告警处理方法流程图，应用于网络管理系统对被管理网络设备的告警分析，该方法包括以下步骤：

[0038] 步骤 s301，网管系统记录被管理网络设备上报的事件，具体包括：网管设备接收来自被管理网络设备上报的事件；网管设备将上报的事件解析，并存入事件库，例如通过 SNMP Trap 事件或 Syslog 事件获取被管理网络设备的事件。其中，网管系统记录被管理网络设备上报的事件之前还可以根据用户需求预先设置告警触发条件，并可以根据用户需求动态修改预设的告警触发条件。该告警触发条件包括但不限于：重复事件触发、关键字触发、闪断事件触发、未知事件触发、未管理设备触发、事件源触发、事件类型触发和时间范围触发中的任意一种触发或者大于等于两种触发的组合。

[0039] 步骤 s302，网管系统判断事件是否符合其上预设的告警触发条件，如符合，则生成告警触发条件对应的告警，并保存该告警，供用户查询；如不符 合，则不产生告警。

[0040] 如图 4 所示，为本发明实施例另一种告警处理方法流程图，本实施例通过将被管理网络设备的所有告警、Syslog 作为事件进行记录，同时定义一系列告警触发条件来实现告警的过滤。其中，事件类型的告警只作为记录用，不需要用户关注，符合告警触发条件的告警需要用户关注。该方法包括以下步骤：

[0041] 步骤 s401，网管系统接收到被管理网络设备的 Trap 告警信息或 Syslog，将其解析得到网管系统可以识别的信息格式。

[0042] 步骤 s402，网管系统将上述告警信息作为事件直接存入事件库中，由于事件只是对客观状态的记录，不分级别，不会象告警那样引起用户关注。

[0043] 步骤 s403，网管系统判断事件库中的事件是否符合告警触发条件，如果符合，则转步骤 s404；如果不符合，则转步骤 s405。其中告警触发条件包括但不限于：

[0044] 重复事件触发：在限定的时间内收到重复事件后触发告警，例如，在 5 秒内接收到了重复事件发送一次告警；在限定的条数内收到重复事件后触发告警，如接收到 100 条某个事件后发送一次告警。

[0045] 关键字触发：根据事件描述中的关键字是否匹配来触发，支持和 / 或关系。例如：接口关闭和启动的事件需要触发告警，则定义的关键字为“接口并且（关闭或启动）”，即关键词中包括“接口”、还包括“启动”和“关闭”中的一项。

[0046] 闪断事件触发：指该事件发生后马上又恢复了，如接口关闭发送了一个事件但马上又发生了一次接口启动的事件，这种事件在正常情况下不会被关注，但如果经常发生则需要关注，生成告警。

[0047] 未知事件触发：未知事件指网管系统不能解析的事件，此类事件超过一定条数则触发一次告警。

[0048] 未管理设备事件触发：未管理设备指事件的发送源未添加到网管系统中，此类告警超过一定条数则触发一次告警。

[0049] 事件源触发：事件源指发生事件的网络设备，可以多种方式定义告警源，例如：根据事件源的 IP 来定义是否触发告警，可以将告警源分类来触发，如定义交换机的事件才触发告警。

[0050] 事件类型触发：根据事件的类型、参数来定义是否触发告警，包括：符合告警类型、参数条件的触发告警；不符合告警类型、参数条件的触发告警。其中事件类型如接口告警、单板告警等；接口告警中的参数为发生告警的接口号；单板告警的参数为发生故障的单板号。

[0051] 时间规则触发：符合时间范围的触发告警，如在下班时间的事件均发告警，反之亦然。

[0052] 当然，上述告警出发条件的具体实现关系可以根据用户需要具体设定。所有告警触发条件均支持正向和取反操作，如事件类型触发，可以是符合事件类型的事件触发告警，也可以是除了符合事件类型的，其他事件都触发告警方式。例如，用户希望将某个交换机 (IP ＝ 1.1.1.1) 除上行接口 (Eth0/0) 外的所有接口类告警屏蔽掉，这个规则涉及多个子规则：事件源触发 (IP ＝ 1.1.1.1)、事件类型触发取反（接口类告警并且接口不等于 Eth0/0)。

[0053] 步骤 s404，产生告警，并存储到告警库中。

[0054] 步骤 s405，网管系统不进行处理。

[0055] 如图 5 所示，为本发明实施例一具体应用流程图，设网管系统预先设定了 N 个告警触发条件，所有告警触发条件既可以单独使用，也可以联合使用来定义一个复合条件。具体过程包括：网管系统接收到被管理网络设备的 Trap 告警信息或 Syslog，将其解析得到网管系统可以识别的信息格式；网管系统将上述告警信息作为事件直接存入事件库中；依次判断该事件是否符合 1 到 N 告警触发条件，符合哪个，则生成对应告警，并存储告警库；如果该事件不符合所有告警触发条件，则不进行处理。

[0056] 如图 6 所示，为本发明实施例一种具有告警处理功能的网络结构图，包括网管系统 100 和被管理的网络设备 200，其中，网管系统 100 对所有的告警应该都有所记录，只是不需要以告警的形式来呈现，事后如果需要审查追踪则可以通过查询历史库找到当时的告警记录。

[0057] 其中，网管系统 100 具体包括：上报事件获取单元 110，用于从被管理网 络设备获取并记录上报事件，具体过程包括：网管系统接收来自被管理网络设备上报的事件，网管系统将上报的事件解析，并存入事件库；告警生成单元 120，用于判断所述上报事件是否符合其上预设的告警触发条件，当符合时，生成该告警触发条件对应的告警，供用户查询；如不符合，则不产生告警。

[0058] 通常情况下，生成的告警信息都应该存储下来，以便用户可以查找，调用，因此网络设备 100 中还包括告警存储单元 130，用于存储所述告警。

[0059] 本发明实施例的关键点就在告警触发上，因此网管系统 100 需要根据用户需求预先设置告警触发条件。其中，预先设置的告警触发条件包括但不限于：重复事件触发、关键字触发、闪断事件触发、未知事件触发、未管理设备触发、事件源触发、事件类型触发和时间

范围触发中的任意一种触发或者大于等于两种触发的组合。当然，上述告警出发条件的具体实现关系可以根据用户需要具体设定。所有告警触发条件均支持正向和取反操作，如事件类型触发，可以是符合事件类型的事件触发告警，也可以是除了符合事件类型的，其他事件都触发告警方式。为了实现扩展，还需要包括告警触发条件更新单元 140，用于根据用户需求动态修改预设的告警触发条件。

[0060] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述的方法。

[0061] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

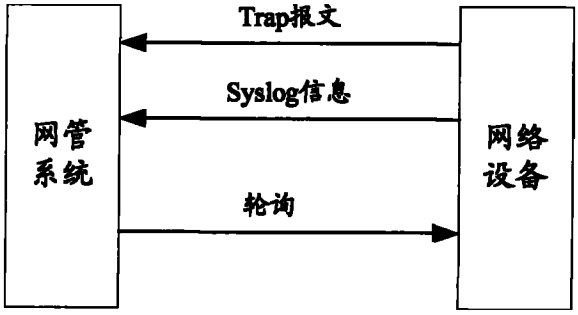

Trap报文
Syslog信息
网管系统
网络设备
轮询

图 1

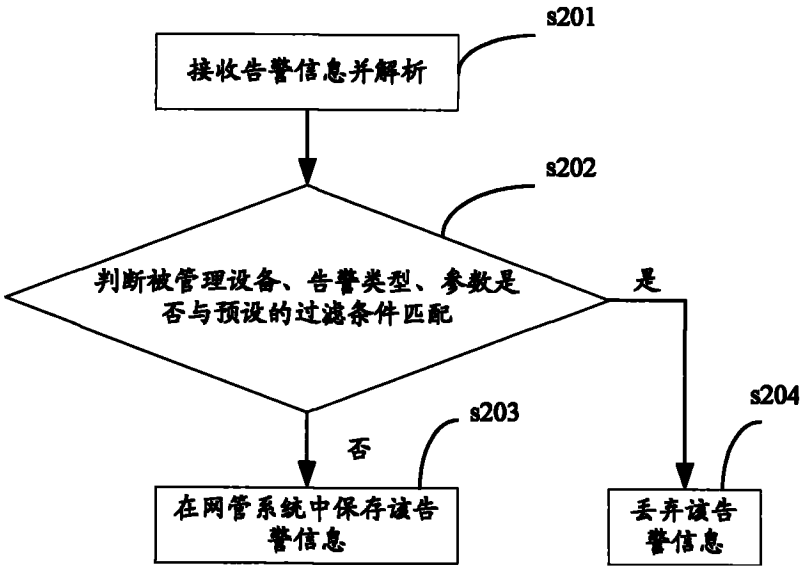

s201
接收告警信息并解析
s202
判断被管理设备、告警类型、参数是否与预设的过滤条件匹配
是
否
s203
s204
在网管系统中保存该告警信息
丢弃该告警信息

图 2

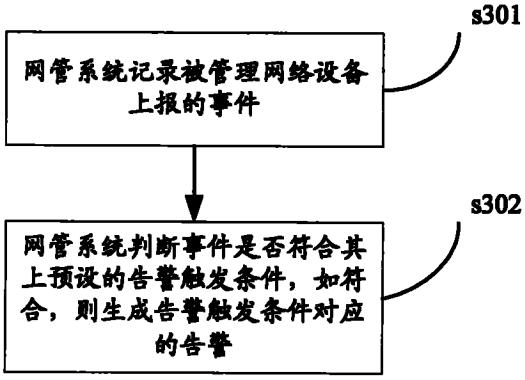

s301
网管系统记录被管理网络设备上报的事件
s302
网管系统判断事件是否符合其上预设的告警触发条件，如符合，则生成告警触发条件对应的告警

图 3

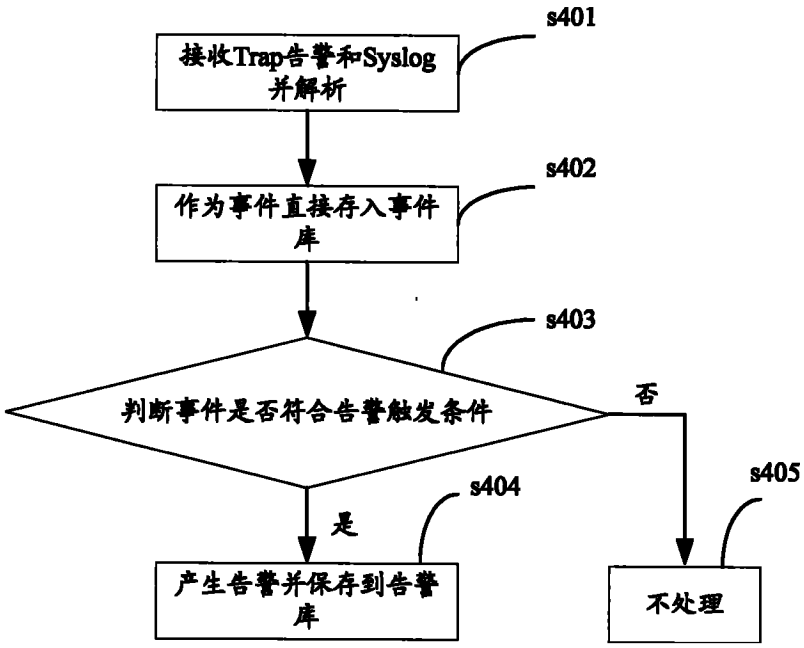

s401
接收Trap告警和Syslog并解析
s402
作为事件直接存入事件库
s403
判断事件是否符合告警触发条件
否
是
s404
产生告警并保存到告警库
s405
不处理

图 4

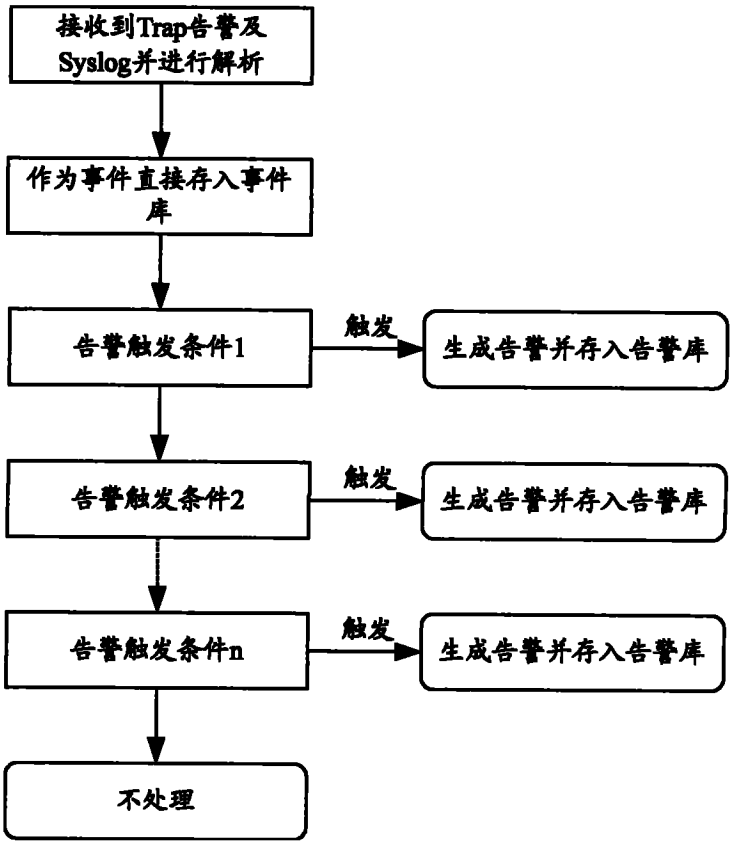

接收到Trap告警及Syslog并进行解析
作为事件直接存入事件库
告警触发条件1
触发
生成告警并存入告警库
告警触发条件2
触发
生成告警并存入告警库
告警触发条件n
触发
生成告警并存入告警库
不处理

图 5

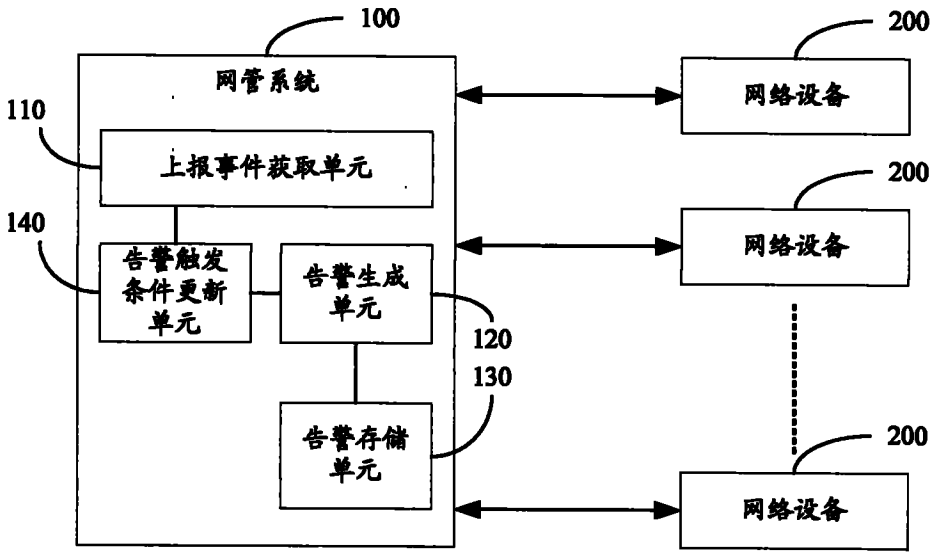

100
网管系统
110
上报事件获取单元
140
告警触发条件更新单元
告警生成单元
120
130
告警存储单元
200
网络设备
200
网络设备
200
网络设备

图 6