

(12) 发明专利

(10) 授权公告号 CN 101159632 B

(45) 授权公告日 2011.01.05

(21) 申请号 200710177817.6

(22) 申请日 2007.11.21

(73) 专利权人 清华大学

地址 100084 北京市海淀区清华园 1 号

(72) 发明人 安常青 杨家海 李星 张辉

黄桂奋

(74) 专利代理机构 北京三高永信知识产权代理

有限责任公司 11138

代理人 何文彬

(51) Int. Cl.

H04L 12/26 (2006.01)

H04L 12/24 (2006.01)

审查员 李东

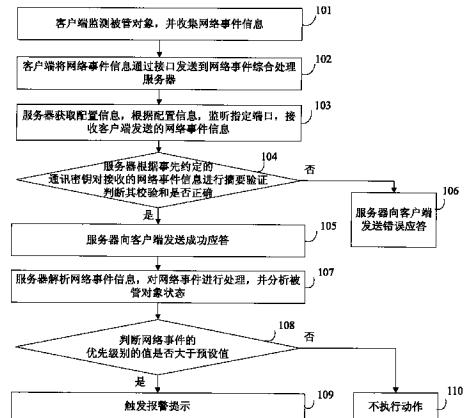
权利要求书 2 页 说明书 10 页 附图 4 页

(54) 发明名称

一种网络事件处理的方法

(57) 摘要

本发明公开了一种网络事件处理的方法，属于计算机网络管理领域。所述方法包括客户端监测被管对象，收集并发送网络事件信息；网络事件综合处理服务器根据网络事件综合处理服务器的配置信息、监听指定端口，接收对应的网络事件信息，验证网络事件信息摘要并返回应答；解析网络事件信息，结合来自多个客户端的事件信息进行综合处理，并分析网络事件信息对应的被管对象的状态；判断网络事件的优先级别值是否大于预设值，如果是，触发报警提示。本发明提供的方法能够支持 IPv4/IPv6 双栈网络，基于 XML 的交换内容的定义有更好的扩展性，更适合于分布式大规模网络管理系统并实现了对来自多个监测客户端的网络事件的综合处理与报警。



1. 一种网络事件处理的方法,其特征在于,所述方法包括:

步骤 A:客户端监测被管对象并收集网络事件信息,通过接口将所述网络事件信息发送到网络事件综合处理服务器;

步骤 B:所述网络事件综合处理服务器根据所述网络事件综合处理服务器的配置信息监听指定端口,接收所述端口对应的网络事件信息,验证所述网络事件信息摘要,如果验证结果正确,向所述网络事件信息对应的客户端返回成功应答;如果验证结果错误,则向所述客户端返回错误应答;

步骤 C:所述网络事件综合处理服务器验证所述网络事件信息摘要正确后,解析所述网络事件信息;

步骤 D:所述网络事件综合处理服务器判断是否已处理与所述网络事件的被管对象相同的事件,如果否,则将所述网络事件的信息作为新记录并插入到压缩事件表中,将所述网络事件插入到原始事件表中,并设置与所述压缩事件表中的新记录关联;如果是,则补充完整所述网络事件信息中被管对象的信息,执行步骤 E;

步骤 E:所述网络事件综合处理服务器根据所述网络事件的被管对象类型、被管对象 ID 和事件类型查找被管对象状态表中的对应表项,如果没有查找出所述表项,则将所述网络事件的信息作为新记录并插入到压缩事件表中,其中,所述新记录的压缩事件 ID 由系统按照增序自动生成,将所述网络事件插入到原始事件表中,并设置与所述压缩事件表中的新记录关联,插入新记录到所述被管对象状态表中,所述新记录的对象信息为所述补充的被管对象的信息,事件类型和事件值为新的事件信息,压缩事件 ID 同新插入到压缩事件表中的记录,如果查找出所述表项,则执行步骤 F;

步骤 F:所述网络事件综合处理服务器比较所述网络事件发生的时间值是否晚于所述表项中的最后更新时间,如果否,则将所述网络事件信息插入到所述原始事件表中,并设置与所述压缩事件表中与所述网络事件的对象和事件类型都相同的事件关联,如果是,则执行步骤 G;

步骤 G:所述网络事件综合处理服务器判断所述网络事件的事件值与所述表项中的事件值是否相同,如果是,则根据压缩事件 ID 更新所述压缩事件表中对应的事件信息的事件发生的时间,将所述网络事件信息插入到所述原始事件表中并设置与所述压缩事件表中的事件关联,更新所述被管对象状态表中对应记录的最后更新时间为新收到的事件的发生时间,如果 否,则将所述网络事件作为新记录插入所述压缩事件表中,其中,所述新记录的压缩事件 ID 由系统按照增序自动生成,将所述网络事件的信息插入到原始事件表中,并设置与所述压缩事件表中的所述新记录关联;更新所述被管对象状态表中对应的表项的事件值和最后更新时间;

步骤 H:所述网络事件综合处理服务器根据处理后的网络事件信息,判断网络事件的优先级别值是否大于预设值,如果是,所述网络事件综合处理服务器触发报警提示。

2. 如权利要求 1 所述的网络事件处理的方法,其特征在于,所述通过接口将所述网络事件信息发送到网络事件综合处理服务器的步骤具体包括:

所述客户端读取所述客户端的配置信息,计算所述网络事件信息摘要,并封装所述网络事件信息;

将封装好的网络事件信息通过接口发送到网络事件综合处理服务器。

3. 如权利要求 1 所述的网络事件处理的方法, 其特征在于, 所述补充完整所述网络事件信息中被管对象的信息的步骤具体为 :

补充完整所述网络事件信息中被管对象的名称、被管对象的地址、被管对象的类型、被管对象的标识。

4. 如权利要求 1 所述的网络事件处理的方法, 其特征在于, 所述报警提示具体包括 : 对话框报警提示或声音播放报警提示。

5. 如权利要求 2 所述的网络事件处理的方法, 其特征在于, 所述网络事件综合处理服务器的配置信息和所述客户端的配置信息具有相同的格式。

一种网络事件处理的方法

技术领域

[0001] 本发明涉及计算机网络管理领域,特别涉及一种网络事件处理的方法。

背景技术

[0002] 网络管理中的事件通常定义为关于网络中正在发生的情况的信息。网络事件通常体现为网络环境中被管理对象上的硬件或软件的故障、安全侵害、性能下降、环境参数变动等。通过 SNMP(Simple Network Management Protocol,简单网络管理协议)等网络管理协议,网络管理系统可以采用轮询的方式查询被管理对象上的相关信息,被管理对象也可以主动向管理系统发出携带相关信息的通知。在网络管理系统中,存在多种网络对象状态的检测手段,如传输层测试、网络层的测试、应用服务层的测试、MIB(Management Information Base,管理信息库)对象检测、域值报警等。

[0003] 随着网络规模的扩大,为了实现网络管理系统的可扩展性,大型网络管理系统的体系结构向着模块化、和分布的方向发展,各个模块分别完成相对独立的功能,但是为了使整个网络管理系统充分发挥效益又要求各个孤立的模块能够协同工作。同时,随着网络应用的发展,光交换等传输网络的发展,IPv6(Internet Protocol Version 6,第六版网络协议)网络逐步建成和投入使用,在网络事件管理方面迫切需要建立能够全面实现 IPv4 和 IPv6 网络事件、IP 网络和传输网络事件、网络层事件和应用层事件的一体化处理机制,在综合分析网络事件的基础上,为管理人员提供真正有用的信息。

[0004] 发明人在实现本发明的过程中发现,现有技术至少存在以下缺点和不足:

[0005] 现有的工作系统,例如,IBM Tivoli,不能够支持 IPv4/IPv6 双栈网络。现有技术提供的方法不支持 IPv4 和 IPv6 网络事件、IP 网络和传输网络事件、网络事件和应用层事件的一体化处理,因此,不能够满足对事件综合分析处理的需求。

发明内容

[0006] 为了支持 IPv4/IPv6 双栈网络,实现网络事件综合分析处理,本发明提供了一种网络事件处理的方法。所述技术方案如下:

[0007] 一种网络事件处理的方法,所述方法包括:

[0008] 步骤 A:客户端监测被管对象并收集网络事件信息,通过接口将所述网络事件信息发送到网络事件综合处理服务器;

[0009] 步骤 B:所述网络事件综合处理服务器根据所述网络事件综合处理服务器的配置信息监听指定端口,接收所述端口对应的网络事件信息,验证所述网络事件信息摘要,如果验证结果正确,向所述网络事件信息对应的客户端返回成功应答;如果验证结果错误,则向所述客户端返回错误应答;

[0010] 步骤 C:所述网络事件综合处理服务器验证所述网络事件信息摘要正确后,解析所述网络事件信息;

[0011] 步骤 D:所述网络事件综合处理服务器判断是否已处理与所述网络事件的被管对

象相同的事件,如果否,则将所述网络事件的信息作为新记录并插入到压缩事件表中,将所述网络事件插入到原始事件表中,并设置与所述压缩事件表中的新记录关联;如果是,则补充完整所述网络事件信息中被管对象的信息,执行步骤 E

[0012] 步骤 E:所述网络事件综合处理服务器根据所述网络事件的被管对象类型、被管对象 ID 和事件类型查找被管对象状态表中的对应表项,如果没有查找出所述表项,则将所述网络事件的信息作为新记录并插入到压缩事件表中,其中,所述新记录的压缩事件 ID 由系统按照增续自动生成,将所述网络事件插入到原始事件表中,并设置与所述压缩事件表中的新记录关联,插入新记录到所述被管对象状态表中,所述新记录的对象信息为所述补充的被管对象的信息,事件类型和事件值为新的事件信息,压缩事件 ID 同新插入到压缩事件表中的记录,如果查找出所述表项,则执行步骤 F;

[0013] 步骤 F:所述网络事件综合处理服务器比较所述网络事件发生的时间值是否晚于所述表项中的最后更新时间,如果否,则将所述网络事件信息插入到所述原始事件表中,并设置与所述压缩事件表中与所述网络事件的对象和事件类型都相同的事件关联,如果是,则执行步骤 G;

[0014] 步骤 G:所述网络事件综合处理服务器判断所述网络事件的事件值与所述表项中的事件值是否相同,如果是,则根据压缩事件 ID 更新所述压缩事件表中对应的事件信息的事件发生的时间,将所述网络事件信息插入到所述原始事件表中并设置与所述压缩事件表中的事件关联,更新所述被管对象状态表中对应记录的最后更新时间为新收到的事件的发生时间,如果否,则将所述网络事件作为新记录插入所述压缩事件表中,其中,所述新记录的压缩事件 ID 由系统按照增续自动生成,将所述网络事件的信息插入到原始事件表中,并设置与所述压缩事件表中的所述新记录关联;更新所述被管对象状态表中对应的表项的事件值和最后更新时间;

[0015] 步骤 H:所述网络事件综合处理服务器根据处理后的网络事件信息,判断网络事件的优先级别值是否大于预设值,如果是,所述网络事件综合处理服务器触发报警提示。

[0016] 其中,所述通过接口将所述网络事件信息发送到网络事件综合处理服务器的步骤具体包括:

[0017] 所述客户端读取所述客户端的配置信息,计算所述网络事件信息摘要,并封装所述网络事件信息;

[0018] 将封装好的网络事件信息通过接口发送到网络事件综合处理服务器。

[0019] 补充完整所述网络事件信息中被管对象的名称、被管对象的地址、被管对象的类型、被管对象的标识。

[0020] 其中,所述报警提示具体包括:

[0021] 对话框报警提示或声音播放报警提示。

[0022] 其中,所述网络事件综合处理服务器的配置信息和所述客户端的配置信息具有相同的格式。

[0023] 本发明提供的技术方案的有益效果是:

[0024] 本发明提供的方法能够支持 IPv4/IPv6 双栈网络,基于 XML 的交换内容的定义有更好的扩展性,更适合于分布式大规模网络管理系统;通信协议采用 MD5 摘要进行信息的认证、校验具有良好的安全性;综合分析来自多个客户端的事件信息,实现 IPv4 和 IPv6 网

络事件、IP 网络和传输网络事件、网络层事件和应用层事件的一体化处理机制，在综合分析网络事件的基础上，为管理人员提供真正有用的信息。实现了网络事件的综合处理与报警，具有良好的可扩展性。事件信息可以根据需要进行传播和信息交换，能够有效地实现信息交互，满足大型网络管理系统中的功能模块相对独立的要求。

附图说明

- [0025] 图 1 是本发明实施例提供的一种网络事件处理的方法流程图；
- [0026] 图 2 是本发明实施例提供的发送网络事件信息的方法流程图；
- [0027] 图 3 是本发明实施例提供的处理网络事件的方法流程图；
- [0028] 图 4 是本发明实施例提供的事件压缩状态转换示意图。

具体实施方式

[0029] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0030] 实施例 1

[0031] 图 1 为本发明实施例提供的一种网络事件处理的方法流程图，本发明实施例所述的网络事件处理的方法步骤如下：

[0032] 步骤 101：客户端监测被管对象，并收集网络事件信息。

[0033] 其中，客户端可以不止一个。比如，可以根据监测类型的不同设置不同的客户端，用于分别监测网络中的被管对象，例如，可以具体为：Trap 事件客户端用于监测被管对象的 Trap 事件，网络故障检测客户端用于监测被管对象故障，传输网监测客户端用于监测传输网，服务监测客户端用于监测网络服务。可以采用数据表的形式分别对客户端和被管对象进行统一的管理。如表 1 所示，本发明实施例提供了一种客户端管理表。

[0034] 表 1

[0035]

字段	含义
客户端 ID	客户端的唯一标识
客户端名称	客户端的名称
IP 地址	客户端的 IPv4 或 IPv6 地址
TCP 端口号	客户端的监听的 TCP 端口号
通讯密钥	客户端使用的通讯密钥

[0036] 如表 2 所示，本发明实施例提供了一种被管对象管理表。

[0037] 表 2

[0038]

字段	含义
ID	被管对象的唯一标识
名称	被管对象的名称
IPv4 地址	被管对象的 IPv4 地址
IPv6 地址	被管对象的 IPv6 地址

[0039] 进一步,如表 3 所示,本发明实施例还提供了一种被管对象接口管理表。

[0040] 表 3

[0041]

字段	含义
接口 ID	接口的唯一标识
接口名称	接口的名称
对象 ID 标识	接口归属的被管对象
IPv4 地址	接口的 IPv4 地址
IPv6 地址	接口的 IPv6 地址

[0042] 步骤 102 :客户端将网络事件信息通过接口发送到网络事件综合处理服务器(以下简称为服务器)。

[0043] 其中,具体的发送过程包括:

[0044] 步骤 102A :客户端在收集到网络事件信息时调用通用的事件转发程序。

[0045] 步骤 102B :读取客户端配置信息。

[0046] 配置信息采用 XML(eXtensible Markup Language,扩展标记语言)格式的配置文件来描述网络事件客户端和服务器的相关信息。

[0047] 其中,客户端和服务器都需要该文件,配置文件的格式都是一样的,配置文件名定义为 EventModules.xml,具体包含以下内容:

[0048] ID :客户端的标识。

[0049] NAME :客户端的名称。

[0050] IP :客户端的 IP 地址。

[0051] LISTENPORT :服务器监听的端口,客户端此参数为空。

[0052] SECRETKEY :客户端与服务器的通讯密钥。

[0053] 具体配置时,客户端和服务器端在配置内容中统称为模块,为了方便读取,配置文件 EventModules.xml 中设置第一个模块是自身并且,可以在配置文件中增加或删除任意多的模块信息。配置文件利用了 XML 技术的优点,具有很好的可配置性。

[0054] 步骤 102C :根据通信协议计算网络事件信息摘要并采用 XML 标签封装网络事件信

息。

[0055] 其中,对网络事件信息通过 XML 进行封装。XML 是可扩展的标记语言,是非专有的可自定义的,可以利用 XML 实现事件的定义与描述而不受任何限制。同时,XML 中的数据是结构化的,即使是相当复杂的事件用 XML 来描述也是一件容易的事情。加上 DTD 或 Schema 的描述作用,能实现对事件信息的严格的自动化处理。

[0056] 客户端和服务器端采用 TCP(Transmission Control Protocol, 传输控制协议)进行通讯,其中通信协议发送内容的格式如表 4 所示。

[0057] 表 4

[0058]

字段	命令字	客户端 ID 长度	客户端 ID	事件信息长度	校验和	事件信息
字节长	32-BIT	32-BIT	不定长	32-BIT	128-BIT	不定长

[0059] 其中,表 4 中的字段内容含义如下:

[0060] 命令字 :0 表示发生了新事件;客户端 ID 长度,因为客户端 ID 不定长,所以需要此字段信息;客户端 ID,用于标识客户端;事件信息长度:因为事件信息不定长,所以需要此字段信息;校验和:为了防止事件信息伪造,对发送的事件信息进行摘要验证;事件信息:表示要发送的网络事件内容。

[0061] 本发明实施例采用了 MD5 摘要(Message-Digest Algorithm 5)进行事件信息验证得到表 4 中的校验和,在具体实现中,如表 5 所示,为利用 MD5 摘要计算校验和时的依据内容,其中,事件信息表示要发送的网络事件内容。

[0062] 表 5

[0063]

字段	命令字	事件信息长度	全零	事件信息	事先约定的通讯密钥
字节长	32-BIT	32-BIT	128-BIT	不定长	128-BIT

[0064] 步骤 102D:将网络事件信息通过接口发送到服务器。

[0065] 步骤 103:服务器获取配置信息,根据配置信息,监听指定端口,接收客户端发送的网络事件信息。

[0066] 服务器获取配置信息,解析配置文件 EventModules.xml 得到客户端的信息,其中配置文件中定义了服务器监听的指定端口。

[0067] 步骤 104:服务器根据事先约定的通讯密钥对接收的网络事件信息进行摘要验证,判断其校验和是否正确,如果是,则执行步骤 105;否则,执行步骤 106。

[0068] 步骤 105:服务器向客户端发送成功应答,并执行步骤 107。

[0069] 步骤 106:服务器向客户端发送错误应答。

[0070] 其中,服务器向客户端发送的应答可以为利用一个整数值表示信息的判断结果,例如:

[0071] 服务器到客户端回应整数 1 表示成功接收到网络事件信息,而且中间没有出过任

何问题 ; 整数 2 表示网络事件信息中有丢失 ; 整数 3 表示摘要验证不对 , 即客户端发送时未使用事先约定的通讯密钥。

[0072] 步骤 107 : 服务器解析网络事件信息 , 对网络事件进行处理 , 并分析被管对象状态。

[0073] 具体处理包括 : 对网络事件信息进行补充以及压缩网络事件信息。为了对网络事件信息进行处理以及对被管对象状态进行分析 , 本发明实施例在服务器上提供了原始事件表、压缩事件表以及被管对象状态表。

[0074] 如表 6 所示 , 本发明实施例提供了一种原始事件表。

[0075] 表 6

[0076]

字段	含义
发生时间	事件发生的时间
收到时间	事件收到的时间
事件发送客户端 ID	事件发送客户端标识
事件类型	事件类型
事件值	事件值
事件的优先级别	事件的优先级别
事件关联对象的类型	事件关联对象的类型
事件关联对象的 ID	事件关联对象的 ID
事件关联对象的名字	事件关联对象的名字
事件关联对象的 IPv4 地址	事件关联对象的 IPv4 地址
事件关联对象的 IPv6 地址	事件关联对象的 IPv6 地址
事件主题	事件主题
事件内容	事件内容

[0077]	压缩事件 ID	与“压缩事件表”中的 ID 属性对应的一个外键 , 表示对应的压缩事件是哪一件
--------	---------	-----------------------------------------

[0078] 如表 7 所示 , 本发明实施例给出了压缩事件表。

[0079] 表 7

[0080]

字段	含义
发生时间	事件发生的时间
事件发送客户端 ID	事件发送客户端标识
事件类型	事件类型
事件值	事件值
事件的优先级别	事件的优先级别
事件关联对象的类型	事件关联对象的类型
事件关联对象的 ID	事件关联对象的 ID
事件关联对象的名字	事件关联对象的名字
事件关联对象的 IPv4 地址	事件关联对象的 IPv4 地址
事件关联对象的 IPv6 地址	事件关联对象的 IPv6 地址
事件主题	事件主题
事件内容	事件内容
事件的状态	事件的状态（打开、关闭）

[0081] 其中，表 6 与表 7 是多对一的关系。

[0082] 如表 8 所示，为本发明实施例提供的被管对象状态表。表中记录了网络事件处理的当前时刻被管对象的状态信息。

[0083] 表 8

[0084]

字段	含义
对象的 ID	被管对象的 ID
对象的类型	被管对象的类型
对象的名字	被管对象的名字
事件类型	发生的事件类型

	事件值	对应的事件值
[0085]	最后更新时间	最后更新时间
	压缩事件 ID	与“压缩事件表”中的 ID 属性对应的一个外键，表示对应的压缩事件是哪一件

[0086] 参见图 3, 步骤 107 具体包括：

[0087] 步骤 107A :服务器判断在被管对象管理表和被管对象接口管理表中是否能查找到网络事件对应的被管对象,如果是,则执行步骤 107B ;否则,表明该网络事件是新对象事件,执行步骤 107J。

[0088] 当服务器在被管对象管理表和被管对象接口管理表中查找不到网络事件对应的被管对象时,说明该网络事件所关联的对象暂时还没有加入到客户端的监测范围内。例如,Trap 事件客户端除了会收到来自被管对象上报的信息外,被管对象外的其他对象(例如设备 B)也会主动向 Trap 事件客户端上报信息,当 Trap 客户端向服务器发送网络事件信息时,服务器在被管对象管理表和被管对象接口管理表就会查找不到关于设备 B 的信息,于是则判断出收到的该网络事件信息为新对象事件。其中,新对象事件是新事件的一种情况。

[0089] 步骤 107B :将网络事件中与被管对象相关的信息补充完整。

[0090] 被管对象相关的信息如被管对象名称,被管对象的 IPv4 地址,被管对象的 IPv6 地址,被管对象的类型、被管对象 ID 等。

[0091] 由于客户端不能把网络事件对应的被管对象的所有信息都发送到服务器上,所以服务器必须根据接收到的网络事件信息进行查找后,将网络事件中与被管对象相关的信息补充完整,查找时采用如下方法:如果网络事件信息中含有被管对象类型,被管对象 ID,则可以根据被管对象 ID 在被管对象管理表和被管对象接口管理表中查找;如果事件信息中只有被管对象 IP 信息,那么首先判断出该 IP 信息中的 IP 是属于 IPv4 还是属于 IPv6,判断出结果后,再根据 IP 信息在被管对象管理表和被管对象接口管理表中进行相应的查找。

[0092] 步骤 107C :查找被管对象状态表,判断根据被管对象类型、被管对象 ID、事件类型进行查找是否能得到对应的表项,如果是,则执行步骤 107D ;否则,表明为新类型事件,执行步骤 107I。

[0093] 其中,新类型事件是新事件的一种情况。

[0094] 步骤 107D :比较网络事件发生的时间值是否晚于查找到的表项中的“最后更新时间”,如果是,表明是非过时事件,执行步骤 107F ;否则,表明是过时事件,执行步骤 107E。

[0095] 步骤 107E :根据网络事件信息插入新的记录在原始事件表中,并与压缩事件表中已有的事件关联。

[0096] 具体的关联是通过设置原始事件表中“压缩事件 ID”为查找到的表项中的“压缩事件 ID”实现。

[0097] 步骤 107F :判断网络事件值和查找到的表项中的事件值是否相同,如果是,表明该网络事件为重复事件,执行步骤 107G,否则,表明该网络事件是新状态事件,执行步骤 107H。

[0098] 其中,因为对象状态发生改变,新状态事件也是新事件的一种情况。

[0099] 步骤 107G :根据“压缩事件 ID”更新压缩事件表中对应的事件信息的“事件发生的时间”;将网络事件信息插入原始事件表中,并与压缩事件表中的事件关联;并更新被管对象状态表中对应记录的“最后更新时间”为新收到事件的“发生时间”。

[0100] 步骤 107H :插入新的记录到“压缩事件表”中,其中“压缩事件 ID”由系统按照增续自动生成,其余的值和收到的网络事件相同;将网络事件信息插入原始事件表中,与压缩事件表中的事件关联;并更新被管对象状态表中对应的表项的“事件值”及“最后更新时间”。

[0101] 步骤 107I :插入新的记录到“压缩事件表”中,其中“压缩事件 ID”由系统按照增续自动生成,其余的值和收到的网络事件相同;将网络事件信息插入原始事件表中,与压缩事件表中的事件关联;插入新的记录到“被管对象状态表”中,其中对象信息为步骤 107B 中补全的对象信息,事件类型及事件值为新的事件信息,“压缩事件 ID”同新插入压缩事件表中的记录。

[0102] 步骤 107J :插入新的记录到“压缩事件表”中,其中“压缩事件 ID”由系统按照增续自动生成,其余的值和收到的网络事件相同;将网络事件信息插入原始事件表中,与压缩事件表中的事件关联。

[0103] 在服务器上具体可以以表格的形式显示处理后的网络事件信息。

[0104] 上述步骤 107A 到 107J,可以理解为是一种对于网络事件的事件压缩。其中,事件压缩是指对于同一个受控对象来说,连续的具有相同事件类型与事件值的事件为重复事件,而造成事件值发生改变的事件是新事件。如图 4 所示,本发明实施例给出了事件压缩转换示意图。事件一开始处于“原始状态”,即为原始事件,状态转换条件如下:

[0105] t1 :事件不跟对象关联或关联对象不在受控范围内。此种情况下,事件是新对象事件,即是“新事件”。

[0106] t2 :事件与某个受控对象关联。通过与对象及其配置信息关联,事件信息得到丰富,进入“完整状态”。

[0107] t3 :事件类型是从没有出现过。事件进入“新类型”。

[0108] t4 :事件类型曾经出现过。事件进入“旧类型”。

[0109] t5 :直接转到“新事件”,即“新类型”事件是新事件。

[0110] t6 :在同类型同对象的事件中,事件发生时间最晚。表示事件是最近才发生的。转入“非过时”。

[0111] t7 :同类型同对象的事件中,事件的发生时间不是最晚的。表示事件不是最近发生的。转入“过时”。

[0112] t8 :事件值与上一次发生的同类型同对象的事件的事件值不同。表示对象的状态发生了改变,转入“事件值不同”,即新状态事件。

[0113] t9 :事件值与上一次发生的同类型同对象的事件的事件值相同。表示对象的状态并没有发生改变。转入“事件值相同”状态。

[0114] t10 :直接转到“重复”状态,终止。因为,过时的事件理解为重复事件。

[0115] t11 :直接转到“新事件”,终止。

[0116] t12 :直接转到“重复”状态,终止。因为事件值相同,所以事件是重复事件。

[0117] 步骤 108 :判断网络事件的优先级别的值是否大于预设值,如果是,表明该网络事件达到报警级别,为报警事件,则执行步骤 109 ;否则,表明该网络事件未达到报警级别,为

一般事件,执行步骤 110。

[0118] 步骤 109 :触发报警提示。

[0119] 其中,该报警提示具体可以以弹出对话框或播放报警声音的形式实现。进一步,在对话框中可以设定相关网页,通过网页查看更为详细的关于报警事件的信息。

[0120] 步骤 110 :不执行动作。

[0121] 本发明实施例提供的方法能够支持 IPv4/IPv6 双栈网络,基于 XML 的交换内容的定义有更好的扩展性,更适合于分布式大规模网络管理系统;通信协议采用 MD5 摘要进行信息的认证、校验具有良好的安全性;实现 IPv4 和 IPv6 网络事件、IP 网络和传输网络事件、网络层事件和应用层事件的一体化处理机制,在综合分析网络事件的基础上,为管理人员提供真正有用的信息。实现了网络事件的综合处理与报警,具有良好的可扩展性。事件信息可以根据需要进行传播和信息交换,能够有效地实现信息交互,满足大型网络管理系统中的功能模块相对独立的要求。

[0122] 本发明实施例提供的方法可以在 2.4GHz 的 CPU,内存 512M 的 Linux 工作环境中实现,网络事件发送、处理以及报警通过 C 语言实现。采用本发明实施例提供的方法实现的系统实际测试环境为中国教育和科研计算机网 CERNET,下一代中国教育和科研计算机网 CERNET2,并实际部署于 CERNET(纯 IPv4 网络),CERNET2(纯 IPv6 网络)和 863 高性能宽带信息网 3TNet(IPv4/IPv6 双栈网络),并具有良好的效果。

[0123] 本发明实施例中的部分步骤,可以利用软件实现,相应的软件程序可以存储在可读取的存储介质中,如光盘或硬盘等。

[0124] 以上所述仅为本发明的较佳实施例,并不用以限制本发明,凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

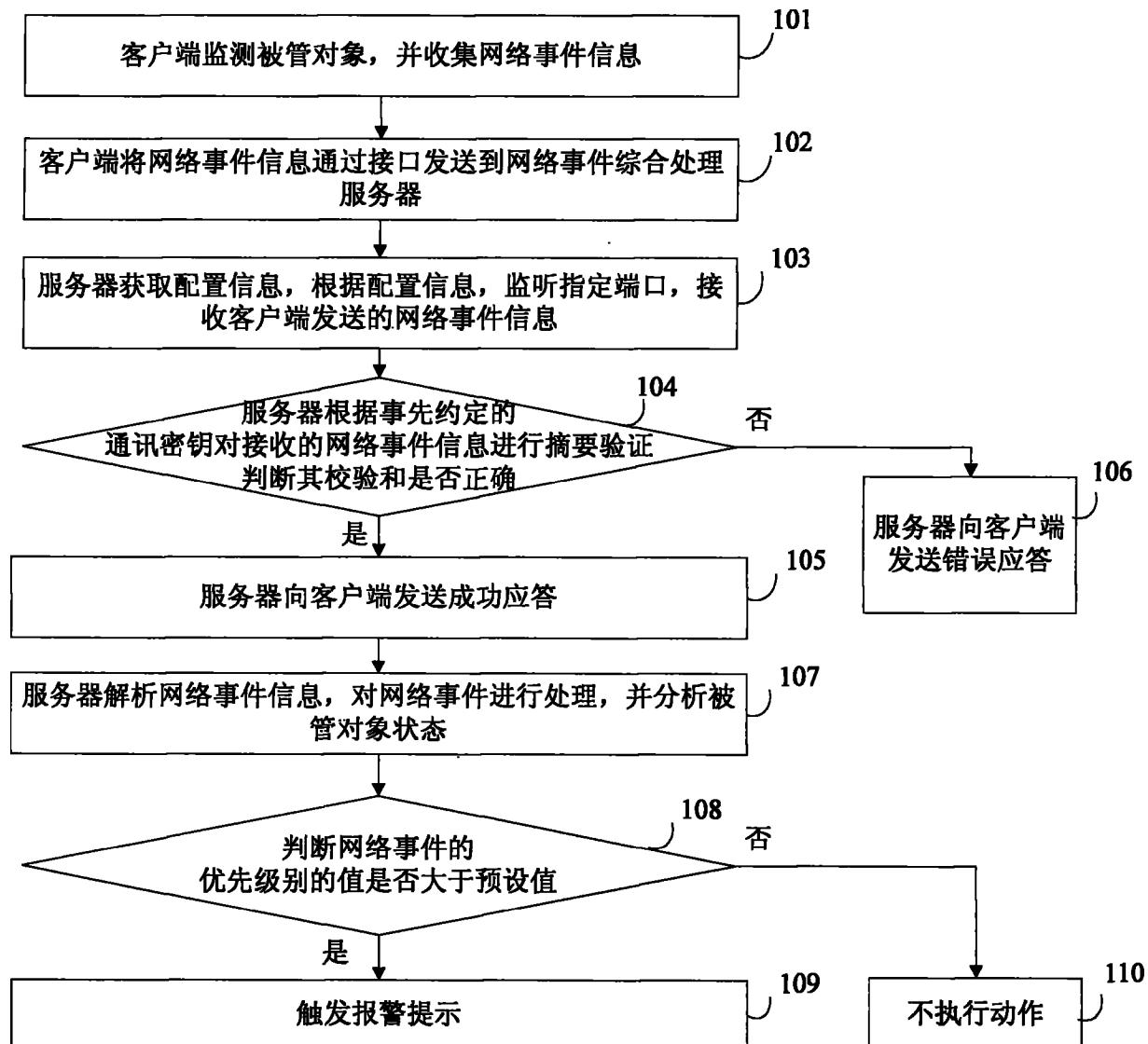


图 1

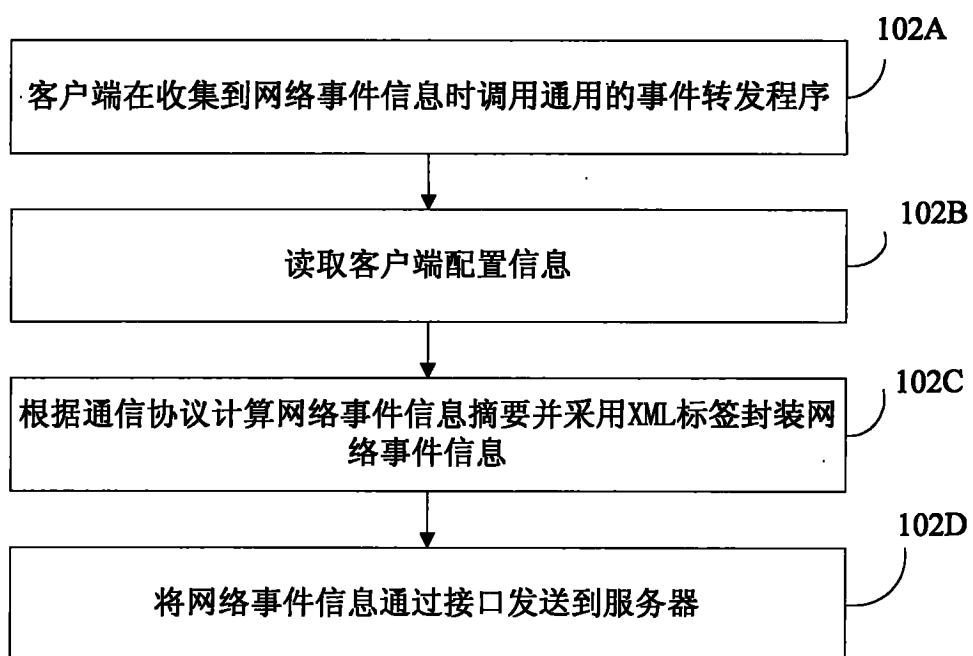


图 2

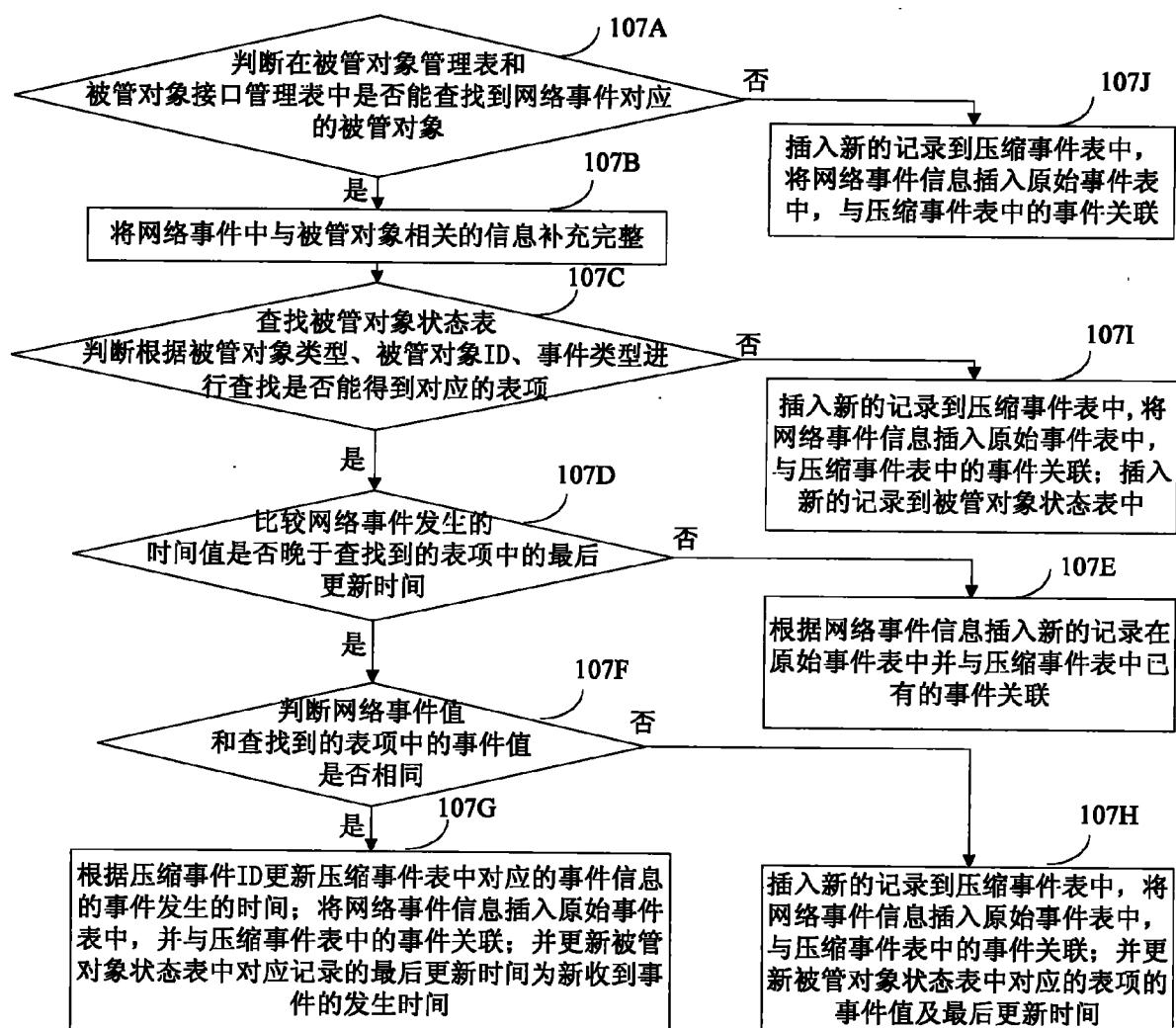


图 3

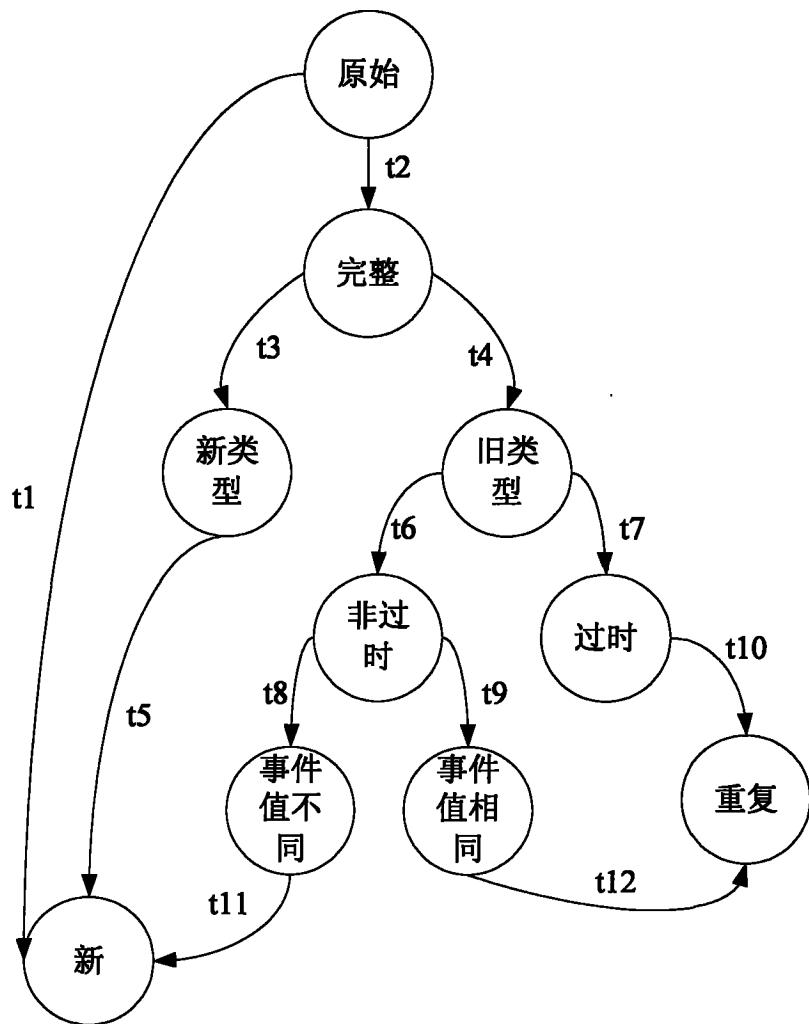


图 4