

[19] 中华人民共和国国家知识产权局

[ 51 ] Int. Cl<sup>7</sup>  
G06F 17/00  
H04L 12/26



# [12] 发明专利说明书

[21] ZL 专利号 01122529.7

[45] 授权公告日 2005 年 3 月 23 日

[11] 授权公告号 CN 1194316C

[22] 申请日 2001.6.28 [21] 申请号 01122529.7

[71] 专利权人 华为技术有限公司

地址 518057 广东省深圳市科技园科发路华为用户服务中心大厦

[72] 发明人 向海洲 吕振峰 陈洪飞

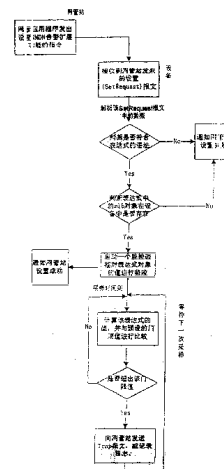
审查员 袁丽颖

权利要求书 2 页 说明书 9 页 附图 2 页

[54] 发明名称 一种计算机网络远程网络监控方法

[57] 摘要

本发明公开了一种计算机网络远程网络监控方法，主要通过 MIB 的表对象中定义一个 MIB 管理对象 PrialarmVariable，所述 PrialarmVariable 为一组至少含有 2 个以上其他 MIB 管理对象的运算组合表达式，网管中心通过发出含有该表达式的报文使管理设备按设定时间启动 RMON 监控进程。该方法支持 SNMP 协议不会浪费网络带宽和消耗网管中心 CPU 资源，优化了网络管理进程，而且对被管设备影响很小。



1、一种计算机网络远程网络监控方法，主要包括如下步骤：

在计算机网络系统中设置有执行简单网络管理协议 SNMP 协议的网管中心；

在所述网络系统中存在有多个由所述网管中心通过设置代理 agent 进行管理的被管理对象；

所述被管理对象为在所述网络系统中可执行 SNMP 协议的子网节点设备或至少一个网络信号传输端口设备；

所述网管中心通过描述多组管理信息表 MIB 表对象来定义被管理对象及其属性，并通过对 MIB 管理对象变量进行监管从而实现对所述网络系统进行监控，其特征在于：还包括如下步骤：

在所述 MIB 的表对象中还定义一组远程网络监视 RMON 告警扩展表，所述告警扩展表包含一个 MIB 管理对象 PrialarmVariable，所述 MIB 管理对象 PrialarmVariable 的语法类型为 OCTECT STRING 类型，所述 MIB 管理对象 PrialarmVariable 为一组至少含有 2 个以上其他 MIB 管理对象的运算组合表达式；

根据实际需要，所述网管中心可发出含有所述运算组合表达式的 set 报文；

所述设备对收到的所述运算组合表达式中的内容进行解析并校验；

经所述设备解析并校验一致的则启动 RMON 监控进程。

2、根据权利要求1所述的网络监控方法，其特征在于：所述运算组合表达式为一组支持四则运算的字符串，其中各MIB管理对象变量采用点加数字格式。

3、根据权利要求1或者2所述的网络监控方法，其特征在于：在启动监控进程后，所述设备在预定时间对所述运算组合表达式计算，并与所述网管中心预设的阈值比较确定是否向所述网管中心发送Trap报文。

4、根据权利要求3所述的网络监控方法，其特征在于：在所述MIB的表对象中还定义一组MIB管理对象PriAlarmStarCycle，所述网管中心通过设置所述MIB管理对象PriAlarmStarCycle来确定终止RMON监控进程的时间和终止RMON监控任务时间长短。

5、根据权利要求1所述的网络监控方法，其特征在于：所述设备为路由器、交换机或网络服务器。

## 一种计算机网络远程网络监控方法

本发明涉及一种计算机网络设备的管理方法，尤其是涉及支持SNMP协议的网络设备的管理。

随着计算机网络规模的不断扩大、网络复杂性的不断提高以及网络异构性的不断增加，网络管理在网络建设、网络运行与网络维护中越来越显得重要。网络管理为监视、控制和管理网络资源提供了一种有效的方法，使计算机网络能够安全、可靠、高效地运行，以达到最优的网络性能。

简单网络管理协议SNMP是基于TCP/IP并在Internet互联网中应用最广泛的网管协议。网络管理员可以使用SNMP监视和分析网络运行情况，通过管理站管理网络、维护网络，但是SNMP的第一代标准SNMPv1（目前所使用的SNMP协议）也有一些明显的不足，如：

- SNMP使用轮询方式采集数据信息，这样浪费了宝贵的带宽资源，增大了网络负荷，在大型网络中轮询会产生巨大的网络管理通讯报文导致网络交通拥挤甚至阻塞，故不适合管理大型网络。
- 不支持管理进程-管理进程的分布式管理，它将收集数据的负担加在网管站上，网络管理站会成为瓶颈。
- 管理信息库MIB是被管设备，如路由器Router、交换机Switch、网络服务器等设备的信息的集合。标准管理信息库MIB-II（RFC1213）和各厂家的专有MIB库主要提供有关设备的数据，如设备端口状态、

流量、错误包数等等。网络管理员只能从这些管理信息库中获得单个设备的局部信息。要想获得一个子网网段的信息是非常困难的一件事情，而在规模越来越大的互联网环境中，人们更需要监控的是一个网段的性能，因此仅仅使用标准MIB获取设备的管理信息已经不能满足管理大型互联网的需要。

为了提高传送管理信息的有效性、减少管理站的负担、满足网络管理员监控网段性能的需求，IETF提出了RMON以解决SNMP在日益扩大的分布式互联中所面临的局限性。

远程网络监视（RMON）为通过端口远程监视网段提供了解决方案。RMON是对SNMP标准的扩展，它定义了标准功能以及在基于SNMP管理站和远程监控者之间的接口。RMON主要实现对一个网段乃至整个网络的数据流量的监视功能，目前已成为成功的网络管理标准之一。

RMON为监控子网的运行提供了一种高效、有用的方法，这种方法能够减少管理者同设备间的通讯流量，简单而有力的管理大型互联网络。它积极主动地监测远程设备，对设备端口所连接的网段上的各种流量信息进行跟踪统计，如某段时间内某网段上报文总数，或发往某台主机的正确报文总数等。它还可以对数据设备进行防范管理，采用RMON技术的设备主动地对网络性能进行诊断并记录网络性能状况，在互联网某处发生故障时（如拥塞）可以把故障信息及时通知管理者，然后由管理者做相应的处理及时准确的排除故障。

通常，RMON的告警组alarm与事件组event一起配合可以实现该功能。例如管理者可以通过配置设备的RMON告警功能，对所关心的设备某个端口的输入字节数ifInOctets管理对象进行监控，如果在一分钟之内该对象统计值超出某个值域范围就向管理站发出警告。启动RMON告警功能后，设备自行对ifInOctets对象进行监控，当发现其超出告警值则发出警告。这样管理者将监控功能转移到设备上执行，避免了对设备各种统计信息的轮询，节省了网络带宽，减轻了网管站的负担。

在实际应用中，RMON告警组alarm虽然能够满足一些设备监控的需要，但是RMON告警组仍然存在着不足，它只能对某一个独立的被管理对象进行监控，如前面提到的端口输入字节数，而对多个管理对象组合信息的监控就无能为力了。例如：如果管理者要对一台设备的某个端口的输入错误百分率进行监控，当该值在十分钟内超过10%时就认为网络出现了某种故障，需要发出告警通知管理人员进行处理，下面接口的输入错误百分率计算表达式：

$$\text{输入错误百分率} = \text{ifInErrors} / (\text{ifInUcastPkts} + \text{ifInNUcastPkts})。$$

这一计算公式包含了三个基本管理对象信息：接口输入错误包数ifInErrors、接口输入单播包数ifInUcastPkts、接口输入非单播包数ifInNUcastPkts。

这种情况下RMON的告警组功能就难以进行监控，只能使用一般的SNMP的处理方法：网管应用程序每隔十分钟一次发出SNMP请求报

文以获取相关信息数据：ifInErrors、ifInUcastPkts、ifInNUcastPkts，然后在本地按照公式计算出结果并将结果与预定值10%进行比较，如果超出预定值则发出告警。这一过程不但浪费了大量的网络带宽，而且消耗了负责网管的设备的CPU时间。在计算机网络中一台网管设备往往要管理上百台的路由器设备，如果每台设备的接口利用率方面的信息都由网管站来负责处理的话，会大大浪费网络带宽，并且影响网管站的分析处理能力，管理站将不堪重负。

另外，RMON还有一个不足：当管理者设置了对某个管理对象的监控告警功能后，只能由管理者主动去取消该告警功能。实际应用中，管理者常常只希望在一段时间内（比如一天内）使用某种监控告警功能，而管理者在管理设备较多的情况下，很有可能忘掉或者不能及时删除该告警功能，这时实际上设备就白白浪费了宝贵的资源来作无谓的监控。

本发明的发明目的是提供一种对现有技术中RMON告警组功能进行改进的且简明有效的网络远程监管方法，该方法支持SNMP协议不会浪费网络带宽和消耗网管中心CPU资源，而且对被管设备影响小。

为了实现上述目的，本发明提供了一种计算机网络远程网络监控方法，主要由如下步骤组成：

在计算机网络系统中设置有执行SNMP协议的网管中心；

在所述网络系统中存在有多个由所述网管中心通过设置代理agent进行管理的被管理对象；

所述被管理对象为在所述网络系统中可执行SNMP协议的子网节

点设备或至少一个网络信号传输端口设备；

所述网管中心通过描述多组 MIB 表对象来定义被管理对象及其属性，并通过对 MIB 管理对象变量进行监管从而实现对所述网络系统进行监控，其特点在于：还包括如下步骤：

在所述 MIB 表的对象中还定义一组 RMON 告警扩展表，所述告警扩展表包含一个 MIB 管理对象 PrialarmVariable，所述 MIB 管理对象 PrialarmVariable 的语法类型为 OCTECT STRING 类型，所述 MIB 管理对象 PrialarmVariable 为一组至少含有 2 个以上其他 MIB 管理对象的运算组合表达式；

所述网管中心已发出含有所述表达式的 set 报文；

所述设备对收到的所述表达式中的内容进行解析并校检；

经所述设备解析并核检一致的则启动 RMON 监控程序。

上述的网络监控方法，其特点在于：在所述表达式为一组支持四则运算的字符串，其中各 MIB 管理对象变量采用点加数字格式。

上述的网络监控方法，其特征不在于：所述设备在预定时间对所述表达式计算，并与所述网管中心预设的阈值比较确定是否向所述网管中心发送 Trap 报文。

上述的网络监控方法，其特点在于：在所述 MIB 的表对象中还定义一组 MIB 管理对象 PrialarmStarCycle，所述网管中心通过设置所述 MIB 管理对象 PrialarmStarCycle 来确定终止 RMON 监控任务的时间和终止 RMON 监控任务时间长短。

上述方法克服了现有技术中的缺陷，提出了一种新的 RMON



告警组的扩展功能，该功能不仅支持网管站为设备记录的任何计数和整数类对象（如流量信息，内存信息等）配置监控功能，而且允许网管站根据需要以表达式形式对多个变量的组合进行配置监控功能，另外还可以控制监控完成的时间：是在进行一段时间后自行结束该监控任务，还是一直监控直到管理者主动取消该功能为止。

本发明可在路由器、交换机等网络设备中得到很好地应用，通过在网管中心运行的网管软件对需要监控的内容进行设置，避免了网管中心的轮询，将部分分析功能转移到路由器、交换机等网络设备上，从而节约了网络带宽，减轻了网管中心的 CPU 系统负担。

下面结合附图进一步说明本发明的实施例

图 1 是本发明实际应用的网络环境；

图 2 是本发明所述方法的工作流程图。

在图 1 中，本发明主要应用于由运行网管应用程序的网管站和大量路由器、网桥等通讯设备组成的计算机通讯网络，在该系统中设置有执行简单网管协议 SNMP 的网管中心，在所述网络系统中存在有许多个由所述网管中心通过设置代理 agent 进行管理的被管理对象，所述被管理对象为在所述网络系统中可执行 SNMP 协议的子网节点设备或至少一个网络信号传输端口设备。

在本发明的实施过程中，首先定义一组管理信息库 MIB 的表对象：RMON 告警扩展表，它与 RMON 告警表管理对象类似，但增加了特殊的管理对象，该表包含一个 MIB 管理对象，姑且称作 PrialarmVariable，它类似于 RMON 告警组的 alarmVariable 对象，

但与 alarmVariable 对象语法类型不同，该对象为 OCTET STRING 类型，当使用者需要对多个变量的表达式进行监控时，可以直接输入表达式，该表达式为一字符串并符合一定的约定规则：支持四则运算，各 OID 变量（OID 代表了 MIB 管理对象）为点加数字格式，如：“.1.3.6.1.2.1.2.2.1.14.1 / (.1.3.6.1.2.1.2.2.1.11.1 + .1.3.6.1.2.1.2.2.1.12.1)” 这就是上面提到的输入错误百分比的计算表达式的输入格式，在设备接收到请求对 PrialarmVariable 对象进行配置的 SET 报文后，对该管理对象的内容（四则运算表达式）进行解析，如果表达式中 OID 变量所代表的管理对象在设备 Agent 中存在且表达式符合四则运算规则，设备将启动监控程序。当采样间隔到达时按照设置要求计算表达式所代表的采样值，并与预先设置的阈值比较，根据一定的策略在超越阈值时发出告警及时通知管理者做防范处理。

另外该 MIB 表对象中还包含一个管理对象 PrialarmStatCycle，网管站可以通过设置该对象用于决定何时终止监控任务，可以做到永久 监视，也可以使该功能在一定时间能自动被取消。

性能管理是网管中的重要内容，其中一个接口的利用率是非常重要的评价指标，但利用率的计算较为复杂：

$$\text{利用率} = ((\text{ifInOctets}_y - \text{ifInOctets}_x) + (\text{ifOutOctets}_y - \text{ifOutOctets}_x)) \times 8 / (y - x) \times \text{ifSpeed}.$$

其中 x, y 时两个不同的查询时刻。

在路由器等通讯设备中可以采用RMON告警扩展功能，这样会很好的利用设备自身的资源来分担网络管理站的负担。

在图2中，本发明的实际应用方式是按照如下工作流程进行的。网管站运行RMON告警扩展网管应用程序，然后管理人员根据需要通过管理程序对相关的设备发出指令（即SNMP setRequest报文，对PriAlarmVariable对象进行设置），在设备得到该指令后，首先获得该指令报文中的数据信息（一个字符串），进行基本的语法检查，判断该数据是否符合语法规则，即是否是一个四则运算的表达式格式，且检查每个表达式中的mib对象的数据在设备中是否可采集，当语法检查通过后，设备根据应用程序对其它RMON告警扩展表的mib对象的设置启动一个监控进程，即每隔一段时间该监控进程计算当前的PriAlarmVariable对象（表达式）的值，然后将该值与网管站预设的一个门限值进行比较，若未超出该门限值，则该次处理结束等待下一次开始；若超出该门限值，则根据网管站预先要求的动作进行处理如向网管站发送Trap实时通知网管站或记录日志以备网管站查询然后等待下一次开始。这样一个监控进程将一直存在直到网管站主动发出命令停止该进程，或者设备根据网管站预先的设置超出有效时间后自动停止该进程。每个设备中可以根据网管人员的需要启动多个这样的监控进程，辅助网管站完成所需要的功能。

利用本发明的RMON告警扩展功能，由网管站分别对每台路由器进行配置所需要的监控指标，如主要接口的利用率情况，由各设备根据配置记录这些指标，当超出某项预设的阈值后，会主动向网管站

---

报告，然后网管站根据报告情况进行处理。例如某接口的利用率经常性超过90%，这就说明该接口所在网络数据量过大需要扩容或者重新分配网络资源了。通过采用本发明的方法大大优化了网络管理。

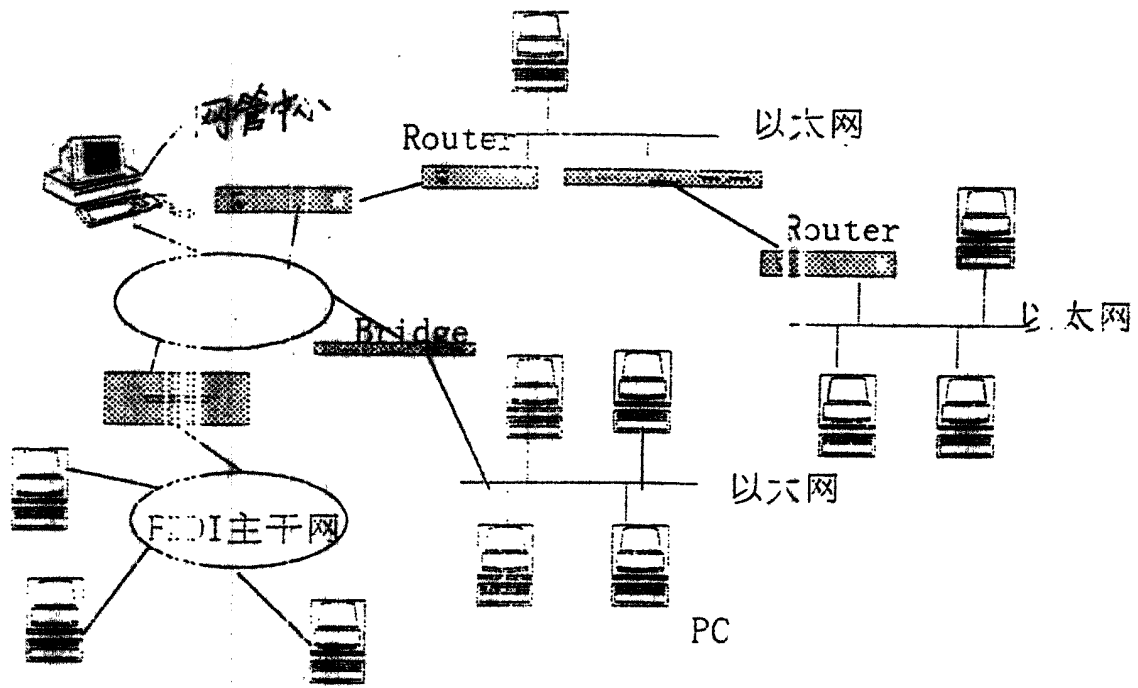


图 1

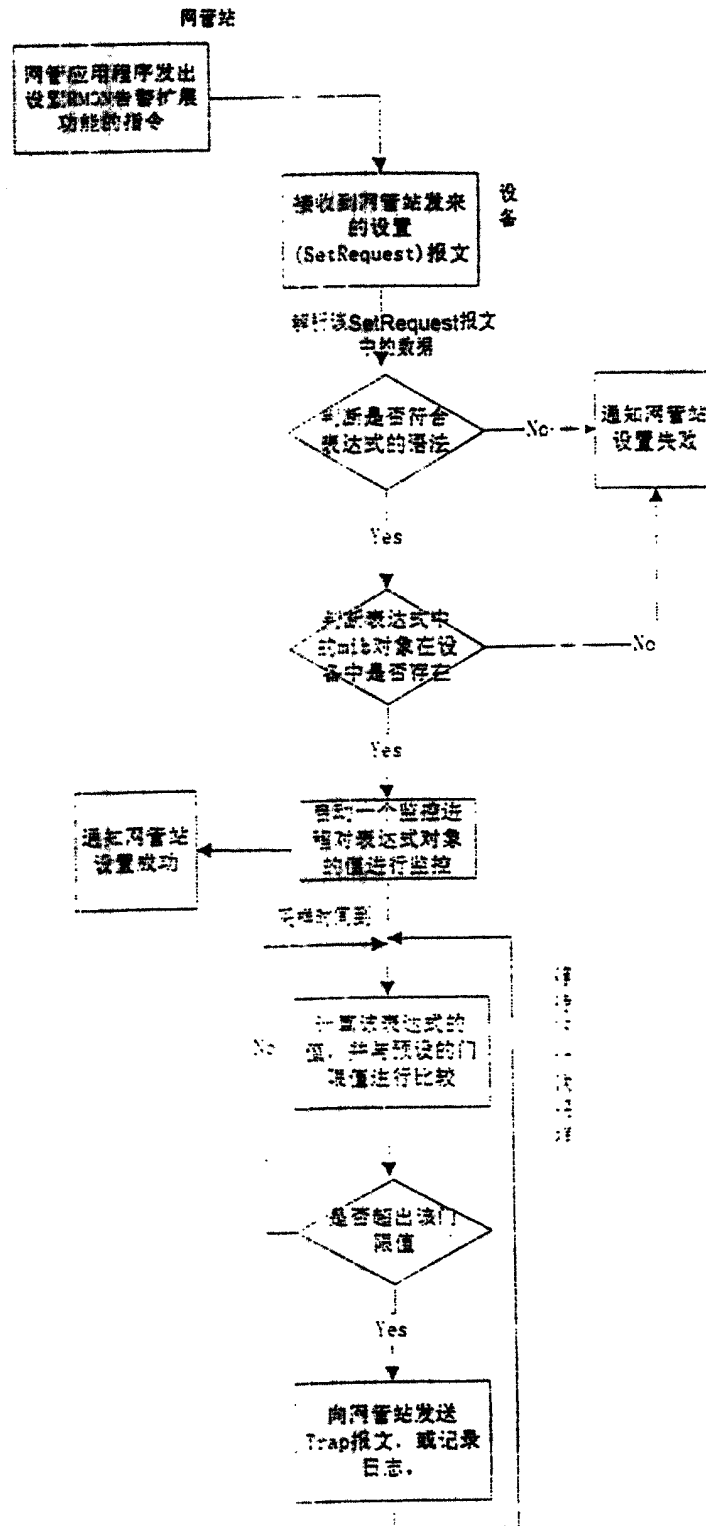


图 2