[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/24
H04L 12/56

[12] 发明专利申请公开说明书

[21] 申请号 200410059593.5

[43] 公开日 2004 年 12 月 1 日

[11] 公开号 CN 1551571A

[22] 申请日 2004.4.15
[21] 申请号 200410059593.5
[30] 优先权
[32] 2003. 4.15 [33] CA [31] 2,425,442
[71] 申请人 阿尔卡特公司
地址 法国巴黎
[72] 发明人 D·A·普罗克斯 C·E·蒂默曼
F·卡茨 M·拉赫尼奥夫斯基
A·扎比赫 M·S·维尔迪

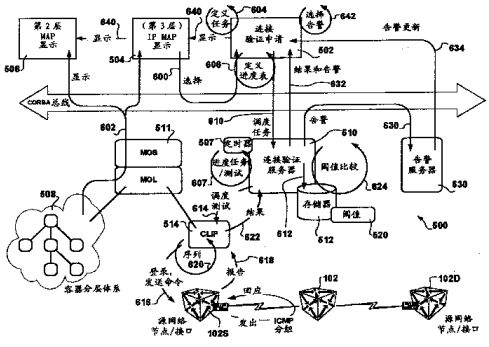
[74] 专利代理机构 北京市中咨律师事务所
代理人 杨晓光 李镇江

权利要求书 2 页 说明书 21 页 附图 13 页

[54] 发明名称 在通信网络管理环境中的集中因特网协议/多协议标签交换连接验证

[57] 摘要

提供一种用于连接验证的结构。该结构包括执行自动的连接验证的连接验证服务器和连接验证应用程序，连接验证服务器和连接验证应用程序在网络管理环境中运行。连接验证任务通连接验验证应用程序定义，从而连接验证服务器被配置。连接验证任务也可以被安排进度。连接验证应用程序还提供连接验证结果的显示。每个连接验证任务的结果可以和期望的连接简档进行比较，以及与连接简档的偏差用来发出告警。包括告警信息的连接验证结果，进一步用于在显示选择的连接验证结果的网络图上突出显示所显示的被管理通信网络实体。通过使用连接验证结构可获得使连接验证测试以减少的操作成本自动进行的优点。



ISSN1008-4274

1. 一种网络管理连接验证结构，包含:

a. 执行自动的连接验证任务的连接验证服务器；和

b. 用于定义连接验证任务，从而配置连接验证服务器，并显示配置验证结果的连接验证应用程序。

2. 如权利要求1所述的连接验证结构，其中连接验证任务被安排进度，并且连接验证服务器执行被安排进度的连接验证。

3. 如权利要求1所述的连接验证结构，其中连接验证应用程序进一步提供连接验证结果的显示。

4. 如权利要求1所述的连接验证结构，其中每个连接验证任务的结果可以和连接简档进行比较，与连接简档的偏差用来发出告警。

5. 如权利要求3所述的连接验证结构，其中包括告警信息的连接验证结果，进一步用来产生网络图，该网络图显示所选择的连接验证结果。

6. 一种创建网络连接验证测试的方法，包括步骤:

a. 定义连接验证任务;

b. 配置连接验证服务器来执行连接验证任务；以及

c. 显示连接验证结果。

7. 如权利要求6所述的创建网络连接验证测试的方法，其中定义连接验证任务进一步包括以下步骤:

a. 通过 NMS 用户接口选择源和目的地 IP 对象对，在它们之间验证连接；以及

b. 规定连接验证进度表。

8. 如权利要求6所述的创建网络连接验证测试的方法，其中定义连接验证任务进一步包含规定应用到连接验证结果的连接验证阈值的步骤。

9. 如权利要求8所述的创建网络连接验证测试的方法，其中规定连接阈值进一步包含为往返延时、抖动、和分组丢失规定阈值。

10. 如权利要求7所述的创建网络连接验证测试的方法，其中选择的 IP 对

象包含路由器、IP接口、和IP地址中的一个。

11. 如权利要求7所述的创建网络连接验证测试的方法，其中通过选择 IP 链路、LSP、和VPN中的一个来选择IP对象对。

12. 如权利要求6所述的创建网络连接验证测试的方法，其中定义连接验证任务进一步包含步骤：配置连接验证参数，该参数包含多个要发出的ping命令、ping分组大小、ping数据填充模式、等待响应的时间、和业务类型中的一个。

13. 如权利要求6所述的创建网络连接验证测试的方法，其中定义连接验证任务进一步包含步骤：配置连接验证参数，该参数包含多个要发出的traceroute命令、traceroute分组大小、traceroute分组数据填充模式、等待响应的时间、和业务类型中的一个。

14. 一种在网络管理环境内执行网络连接验证的方法，包含步骤：

a. 执行被安排进度的连接验证；

b. 将连接验证结果和阈值进行比较；以及

c. 如果连接验证结果达到该阈值，发出告警。

15. 如权利要求14所述的执行网络连接验证的方法，进一步包含步骤：在计算机可读介质上存储连接验证任务用于以后的访问和执行。

16. 如权利要求14所述的执行网络连接验证的方法，进一步包含步骤：按照连接验证任务和连接验证结果之一突出显示至少一个IP对象。

17. 如权利要求16所述的执行网络连接验证的方法，其中突出显示的对象是OSI第2层和OSI第3层对象中的一个。

18. 如权利要求14所述的执行网络连接验证的方法，其中执行被安排进度的连接验证的方法步骤进一步包含步骤：周期地执行连接验证测试。

19. 如权利要求14所述的执行网络连接验证的方法，其中执行被安排进度的连接验证的方法步骤进一步包含步骤：发出ping命令和traceroute命令中的一个。

20. 如权利要求 14 所述的执行网络连接验证的方法，进一步包含步骤：在计算机可读介质上存储历史连接验证结果用于以后的访问。

在通信网络管理环境中的集中因特网协议/多协议标签交换连接验证

技术领域

本发明涉及通信网络管理和服务提供，尤其是，涉及用于通信网络管理环境中的集中因特网协议/多协议标签交换连接验证的方法和设备，来确保遵守服务等级协议。

背景技术

在因特网协议（IP）/多协议标签交换（MPLS）通信领域中，已知通过使用由“ping”命令和“traceroute”命令提供的功能来验证两个数据网络节点是否可以互相到达。在因特网工程工作组请求注解（RFC）1147中描述了 ping 和 traceroute 命令功能性规范的实施，其在此引入作为参考。ping 和 traceroute 命令的相关概念的简述如下:

本领域普通技术人员将理解，数据通信网络根据 IP 协议和/或 MPLS 协议传送数据分组是根据存储和转发规则执行的。在通信网络的每个数据网络节点上，分组通过输入端口被接收、存储，并实时确定输出端口，并且分组通过确定的输出端口被转发。实时端口确定称为路由功能并由路由器网络元件执行。输出端口的实时确定按照各种因素进行，这些因素包括: 包含在分组报头中的目的地寻址信息、转发类型关联、分组业务区分、在网络节点之间的互连链路的工作状态、链路上的传输带宽可用性、在路径中的数据网络节点上的分组处理带宽可用性等。

本领域普通技术人员将理解，数据通信网络根据 IP 协议传送数据分组是根据尽力型分组传输规则执行的。尽力型规则不保证数据分组将到达它们的目的地，不保证有界的分组到达等待时间，不保证有界的分组到达抖动等。事实上，

规定相同的源网络地址和相同的目的地网络地址的分组没必要遵循数据通信网络中的相同传输路径，这即是本领域已知的松散源路由。

上述的实时输出端口确定可导致这样的情况，其中建立分组传输环路。每个IP 分组将生存时间（TTL）规范携带在它的报头中，该生存时间（TTL）规范是由发送分组的源数据网络节点（或者在用户网络和服务提供商网络之间的边缘的网关）初始设置的整数报头字段值，并且由转发该分组的每个数据传输节点减1。当 TTL 值达到零（0）时，该分组被丢弃。

尽管简单，但是该方法对 IP 网络设计施加了大量压力以保证在源数据网络节点和目的地数据网络节点之间只有少量的数据传输节点被经过，从而只有少量的互连链路被经过。互连链路的物理实现可变并可以包括附加的数据/分组传输协议-因此从连接验证的观点来看，在两个相应数据传输节点上的两个接口之间的数据通信网络的基础结构被称作一“跳”以对其进行抽象。

如上所述，尽力型分组传输规则不保证有界的分组到达等待时间。等待时间是分组穿过从其源数据网络节点到其目的地数据网络节点的通信网络所花费的时间量。等待时间典型地用毫秒计量并且包括与物理互连链路上的分组的物理传送相关的物理数据传输延时，以及当分组存储在处于源网络节点和目的地网络节点之间的传输路径中的传输网络节点中时，在等候确定输出端口时分组所引起的分组处理延时。

如上所述，尽力型的分组传输规则不保证有界的分组到达抖动。抖动是分组到达之间的延时的变化的量度，并且涉及由通常与在提供数据业务中所使用的数据流相关的一组单个的数据分组引起的一组延时的标准偏差的量度。

服务提供，超出了本说明书的范围，其取决于所提供的结果的服务质量。服务质量是用于特定数据业务的带宽、到达延时和抖动规范的组合，该特定数据业务在给定的互连通信网络基础结构上端到端提供。

本领域技术人员可以理解，为了提供高的服务质量分组传输，已经开发了MPLS 传输协议。虽然，与在物理互连链路上的物理分组传播有关的延时只能减少到一定程度，但 MPLS 技术提供：在互连链路上的带宽预留，用以确保资源可用性；严格的（预先规定的）路由/传输路径，用以最小化沿着该路径的分组处理

延时；和强化的多传输层交换，使得路径中的交换网络节点上交换延时最小化。具有相同源网络地址和相同目的地网络地址的分组可以遵循不同的传输路径，这取决于用于每个分组的服务等级协议（SLA）规范。

在 MPLS 环境中遵守服务等级协议，并且需要在本发明的说明书中所提出的尽力型 IP 环境中遵守服务等级协议规范。

ping 和 traceroute 功能的执行包括至少一个单独回应返回因特网控制报文协议（ICMP）分组的返回传送，在源网络节点和目的地网络节点之间的数据通信网络中的分组探测，用以验证其间的连接。

参见图1，由 ping 探测分组验证连接的程度与可达性相关。ping 探测分组携带 TTL 值，因此可达性包括：一种评估，该评估是关于在 TTL 届满之前是否存在互连链路的至少一个边界序列，该边界序列可以被在源网络节点和目的地网络节点之间传送的分组经过。需要强调的是，每个 ping 探测分组测试在一对预先规定的源和目的地网络节点间的连接。

除了测试可达性外，每个 ping 探测分组还标有时间戳值，该时间戳值对应于由源网络节点发出 ping 探测分组的时间，使得当在源网络节点上 ping 探测分组返回时能够计算总返回传输延时。在发送一组 ping 探测分组中，总返回传输延时的相应组用来确定：最小延时，最大延时，平均延时（用毫秒计），以及抖动。确定的最小延时、最大延时、平均延时和抖动称为分组传输统计量。

正如所知道的，通过使用 traceroute 分组执行的连接验证的程度，与在源和目的地网络节点之间的路径中的网络节点发现有关，如图2所示。执行 traceroute 功能使用要去往目的地网络节点、并具有增大的 TTL 值的 ICMP 回应返回分组的组。在 TTL 值减小到零时 traceroute 分组被返回到源网络节点，因此在发送 traceroute 分组中使用增大的 TTL 值，以沿着源网络节点和目的地节点之间的路径发现进一步增加的中间传输网络节点。

参照图3，对于源路由标签交换路径（LSP）预先建立的路径，由于 traceroute 分组在通过 LSP 传输时被封装，沿着 LSP 传输路径进一步增加的物理网络节点可以不返回 traceroute 分组，TTL 值只在返回 traceroute 分组的 LSP 的末端减少。当然 traceroute 分组会被在 LSP 末端之外的网络节点返回。

在尽力型的 IP 环境中，由于在源和目的地网络节点之间的网络节点上分组处理情况动态地变化，并不能保证所有的 traceroute 分组被相同地路由。期望通信网络的稳定性程度，尽管无法保证，当 traceroute 分组以相对快速连续发送时，该稳定性程度将导致 traceroute 分组的组大体上遵循相同的传输路径。

在返回的 traceroute 分组中保留的信息用来提取传输延时信息。统计信息从 traceroute 分组的连续序列中得到。因此可以为通信网络中一对网络节点之间的每个确定的传输路径提供传输延时和抖动简档。这些延时和抖动简档的范围可用于得到每跳统计量，该统计量留给解释该统计信息的高层应用，高层应用超出了本说明书的范围。

提供了 ping 和 traceroute 功能的概括后，必须强调的是，ping 和 traceroute 分组从源网络节点发出，并返回到相同的源网络节点。结果统计量也可由源网络节点并在源网络节点获得。

服务提供商包括给用户提供通信服务的组织和通信网络基础结构。服务包括尽力型分组传输、MPLS 分组传输、以及分化的服务例如支持虚拟专用网络（VPN）连接的虚拟局域网（VLAN）。

目前服务提供商广泛地使用 ping 和 traceroute 功能来在非常有限的基础上验证连接。典型地，操作管理人员需要物理地和人工地通过命令行接口（CLI）在每个远端源网络节点上登录，从即时规定的人工寻址网络节点中发出必要的 ping 和／或 traceroute 命令，捕获控制台输出，并从远端源网络节点检索出输出。

在服务提供商管理的通信网络中，更重要的是验证单独的路由器之间的连接。路由器包括物理路由器通信网络节点和与交换通信网络节点相关的虚拟路由器。参照图4，显示了提供 VPN 业务 VPN1和 VPN2的五个全网格路由器 R1，R2，R3，R4 和 R5。用于位置1和位置3之间的 VPN1的连接验证可以两个步骤人工执行：ping ／traceroute 测试 T1从 R1向 R3运行，第二 ping／traceroute 测试 T2从 R3向 R1 运行。每次 ping／traceroute 测试运行时，操作者必须登录源路由器，运行 ping ／traceroute 测试，并检索出结果。

如果在所有对等路由器之间都需要连接验证，在 VPN1中将需要更多的测试步

骤：ping／traceroute测试T3验证从位置2到位置3的连接，需要另一个ping／traceroute测试来验证从位置3到位置2的连接，其他两个ping／traceroute测试必须在位置1和位置2之间进行。

操作者必须执行更多的ping／traceroute测试用于其他VPN，例如在位置2和位置4之间的VPN2。

以两个单独的步骤执行在每对位置之间的连接验证时，对于操作管理人员而言，来自哪个路由器的哪个路由器IP地址和VLAN标识符（VPN1/VPN2）被使用是不明显的。这种操作者参与的水平是不够的，因为CLI命令输入是非常耗费时间的、复杂的、并容易出错的过程，这导致由服务提供商引发巨大操作开销。特别地，人工命令输入使得在这样的环境下执行连接验证是不可能的也是来不及的，在该环境中大量的用户利用经大量链路互连的大量通信网络节点的基础结构向由服务提供商服务的相应的大量VPN进行预订。有意义的统计量需要从在相对短期内执行的大量的ping／traceroute测试中得到。

分组业务模式在一段时间内变化，并典型地在一天的时间内循环和在一周内循环。因此，对于用户和服务提供商而言，在高峰时间（营业时间和晚上）和高峰工作日（工作日和周末）期间执行连接校证是重要的。因此，显然如果人工操纵的连接验证是耗费时间的，由于包含巨大的操作开销，在测试窗口中的人工连接验证则变得不可能。连接验证测试数随着用于每个VPN的位置组合数而增加，使得连接验证更加复杂和耗费时间。

最接近现有技术和网络拓扑发现有关，并包括：

现有技术的、由Keeler，Jr.等人申请的、在2002年12月31日公开的、题目为“System and Method for Collecting Connectivity Data of an Area Network”的美国专利6，502，130 B1描述了一种系统和方法，该系统和方法从互连多个计算机设备的局域网中收集动态连接数据。动态连接信息在数据仓库中与静态网络信息组合，与各种用户和他们的特权相关。存储在数据仓库中的组合数据允许识别出每个用户和用户的各种特权，每个用户和用户的各种特权被连接端口关联。使用在简单网络管理协议（SNMP）中的命令来收集连接数据。SNMP命令查询所有网络设备例如集线器、路由器、和到其他网络的网关来获得端口连接信息，例如

被每个网络用户使用的端口的标识。尽管具有创造性，但由 Keeler Jr. 等人提出的解决方案只实现了支持记费应用的开放系统互连（OSI）第2层和第1层的互连发现，该记费应用用于预订漫游网络访问业务的用户。Keeler Jr. 等人并没有解决关于确保实时遵守服务等级协议的问题。

现有技术的、Sharon 等人申请的、2001年3月20日公开的、题目为“Automatic Network Topology Analysis”的美国专利6，205，122 B1描述了一种用于物理网络拓扑的自动检测的方法和系统，它是通过使来自连接到网络上的计算机的信息相关实现的。虽然有创造性，但是由 Sharon 等人提出的解决方案没有解决关于确保实时遵守服务等级协议的问题。

现有技术的、Iyer 申请的、2002年5月28日公开的、题目为“System and Method to Discover End Node Physical Connectivity to Networking Devices”的美国专利6,397,248 B1描述了一种用于确定网络中端节点和联网设备之间的物理连接的装置和方法。Iyer 解决了关于 SNMP 协议不能确定在端节点和联网设备之间的物理连接的问题。虽然具有创造性，但是由 Iyer 提出的解决方案并没有解决关于确保实时遵守服务等级协议的问题。

现有技术的、Wood 申请的、2002年6月11日公开的、题目为“Method and Apparatus for Determining Accurate Topology Features of a Network”的美国专利6，405，248 B1描述了一种用于确定利用源地址表的特定网络的准确拓扑特性的方法。该解决方案提出了以规则的间隔从每个网络交换节点的每个端口获得源地址表信息，来确定何时得知特定源地址以及何时丢弃。源地址信息被用于发布地址解析协议（ARP）查询以确保源地址信息是有效的。虽然具有创造性，但由 Wood 提出的解决方案没有解决关于确保实时遵守服务等级协议的问题。

现有技术的、Shurumer 等人申请的、1999年10月26日公开的、题目为“Communications Network Monitoring”的美国专利5，974，237描述了一种专有方法，用于监视包含诸如交换机的多个节点设备、和诸如光纤链路的链路设备的通信网络，其中节点设备的单个特定于厂商的部件的专用性能参数用来为节点设备确定总体专用性能参数。通过比较用于单个网络单元的相同的专用性能参数，不同类型的专用网络单元的性能相互之间可以进行比较。可被监视的参数包括服务

质量、信元丢弃、信元丢失、和网络性能的其他测量值。通过大量节点设备和链路设备的连接跟踪被用于使用专用装置以提供拓扑发现中。虽然具有创造性，但由Shurumer等人提出的解决方案没有解决关于确保实时遵守服务等级协议的问题。

其它开发还包括，现有技术的、Grant等人申请的、2001年4月24日公开的、题目为“Telecommunications Network Management System”的美国专利6，222，827 B1描述了一种用于管理同步数字体系（SDH）网络的系统，并提出跟踪和处理支持规定用于建立数据管道的连接参数的网络相关数据。该解决方案涉及网络管理系统，其形成网络概观和它的状态，从中，系统向每个传输设备提供配置命令以便所有的配置变化可以显著更快速地执行。虽然具有创造性，但由Grant等人提出的解决方案没有解决关于确保实时遵守服务等级协议的问题。

减少操作成本对服务提供商是重要的。解决这些顾虑对大型的和复杂的服务提供商IP/MPLS通信网络是尤其重要的。因此，需要解决上述的问题。

发明内容

根据本发明的一方面，提供一种用于连接验证的结构。该结构包括执行自动连接验证的连接验证服务器、和连接验证应用程序，连接验证服务器和连接验证应用程序运行在网络管理环境中。

根据本发明的另一方面，通过连接验证应用程序来定义连接验证任务，从而配置连接验证服务器。

根据本发明的另一方面，连接验证任务被安排进度，并且连接验证服务器执行被安排进度的连接验证。

根据本发明的另一方面，连接验证应用程序还提供连接验证结果的显示。

根据本发明的另一方面，每个连接验证任务的结果可以与期望的连接简档进行比较，并且与连接简档的偏差可以用来发出告警。

根据本发明的另一方面，包括告警信息的连接验证结果，还用于产生显示所选的连接验证结果的网络图。

使用该结构来以减少的操作成本执行自动安排进度的连接验证可获得优点。

附图说明

．本发明的特征和优点在下面结合附图对优选实施例的详细描述中将会变得更加清楚，其中：

图1是显示了在源和目的地节点之间人工执行的 ping 连接验证测试的示意图；

图2是显示了在源和目的地节点之间人工执行的 traceroute 连接验证测试的示意图；

图3是显示了在经过LSP的源和目的地节点之间人工执行的 traceroute 连接验证测试的示意图；

图4是显示现有技术人工虚拟专用网络连接验证的示意图；

图5是根据本发明的典型实施例显示了连接验证结构的元件的示意图；

图6是根据本发明的典型实施例显示了参与到 VPN 中的网络节点和要执行的连接验证测试的全网格双向组的示意图；

图7是显示了根据本发明的典型实施例执行的连接验证的示意图；

图8是根据本发明的典型实施例显示了使得操作管理人员能够在网络管理环境中集中处理 ping 连接验证任务的人机界面视图的示意图；

图9是根据本发明的典型实施例显示了连接验证任务状态的状态示意图；

图10是根据本发明的典型实施例显示了使得操作管理人员能够定义 ping 连接验证任务的人机界面的示意图；

图11是根据本发明的典型实施例显示了使得操作管理人员能够定义 traceroute 连接验证任务的人机界面的示意图；

图12是根据本发明的典型实施例显示了图8中所示的、使得操作管理人员能够在网络管理环境中集中处理 traceroute 连接验证任务的人机界面的另一视图的示意图；

图13是根据本发明的典型实施例显示了使得操作管理人员能够为连接验证任务定义进度表的典型人机界面窗口的示意图；以及

图14是根据本发明的典型实施例显示了使得操作管理人员能够为连接验证任务定义阈值的典型人机界面窗口的示意图。

应当注意，在附图中相同的特征用相同的标号表示。

具体实施方式

图5根据本发明的典型实施例显示了在集中通信管理环境中使用的连接验证结构500。连接验证应用程序502使用通过IP图应用程序504和/或第2层图应用程序506提供的网络图，使得能够从由网络管理系统（NMS）的被管理对象服务器（MOL）511通过容器层次体系508跟踪的被管理网络节点组中选择600显示的602源102S和目的地102D网络节点。

所选择的600源102S和目的地104D网络节点用来定义604连接验证任务。尽管一旦连接验证任务被定义604，连接验证任务即可被调度610来立刻执行，用于连接验证任务的进度表也可以被定义606。连接验证任务定义604包括：规定连接验证参数，该参数包括要执行的连接验证测试的类型和数量；以及可选地规定应用到返回的连接验证结果的阈值520（如下面所述）。

根据本发明典型实施例的另一个实现方案，通过规定（600）源102S和目的地102D网络节点对，定义一对双向连接验证测试。

NMS系统提供被管理的通信网络实体的集中网络管理视图，这些实体包括：路由器、IP链路、IP接口、未被管理路由器的IP地址、标签交换路径（LSP）、VPN等。根据本发明典型实施例的另一个实现方案，因特网协议（IP）和在容器层次体系508中的第3层源和目的地被管理实体对象实例可以从容器层次体系508本身中选择（600）。

通过选择（600）VPN被管理实体，规定参与网络节点102组。根据本发明典型实施例的另一个实现方案，选择600网络节点被管理实体组，定义了600全网格双向连接验证任务，以便在选择的组中的所有网络节点102对之间执行相应的连接验证测试。图6显示了5个选择的网络节点102的示例组，以及在其间执行的相应的双向连接验证测试，而不管其间是否提供物理全网格互连链路（即使物理全网格互连链路被提供分组传输协议，例如在此引入作为参考的生成树协议，指明某条物理链路作为备用链路）。为了清楚起见，对于所选组中的N个网络节点102，自动地定义604 N(N-1)/2个双向连接验证任务来调度614在N(N-1)/2对选择的

(600)网络节点102之间的N(N-1)个单向连接验证测试。操作管理人员具有从多个连接验证测试中收集统计量的手段。因此，一旦选择被管理的VPN实体，操作管理人员具有通过单击容易地调度610 VPN连接验证任务来验证整个VPN连接的手段。

每个连接验证任务可通过连接验证服务器510调度610来立即执行，或者存储612在与连接验证服务器510相关的储存库512中用于延时和/或重复的调度610。该连接验证服务器510基于与其有关而规定的进度信息启动连接验证任务。连接验证服务器510在定义的进度表606中规定的合适时间，或者如果在相应的连接验证测试中规定的源被管理实体(102S)空闲时一旦请求马上通过命令行接口处理器(CLIP)514排队连接验证测试用于调度614。安排进度的连接验证任务始终具有优先级。

安排进度的连接验证任务具有增加的功能，该功能允许它们排队用于重复执行，提供在规定时间验证连接并因而从获得的重复结果中产生总的统计量的能力，该统计量支持确定是否满足用户的SLA或者在通信网络中是否存在故障。

根据本发明的典型实施例，提供一种用于调度多个连接验证任务的机制。连接验证服务器510包括定时器507。连接验证服务器510浏览607关于排队的连接验证任务而规定的安排进度信息(606)，以便在规定的时间调度614连接验证测试。

CLIP处理器514接管发出616连接验证测试命令(典型地为CLI命令，但本发明不限于此)到空闲的源被管理实体(102S)，并且在交互会话中检索出618连接验证结果，其中CLIP处理器514登录源被管理实体(102S)。因此CLIP处理器514提供用于连接验证测试结果的中央收集的手段。

CLIP处理器514序列620命令发出以免使通信网络被ICMP业务所过载。CLIP处理器514接下来不发出命令给被管理实体，直到发出的最后一个命令已经完全执行(并且结果已经检索回)而不管为连接验证任务规定的606进度表。

连接验证结果提供622给连接验证服务器510，该服务器可以将连接验证结果与关于连接验证任务而规定的阈值520进行比较624，该连接验证任务评价遵守相应的SLA协议。当到达阈值520时，通过告警服务器530产生630告警。该结果和告警信息也可以传播632给连接验证应用程序502。提供632给连接验证应用程序

502的告警信息可随后被告警服务器530更新634。

根据本发明典型实施例的另一个实现方案，每个连接验证结果与包含至少两个阈值520的阈值简档（520）进行比较，多个阈值用来实现多级告警严重性。

随后提供632连接验证结果给连接验证应用程序502。连接验证应用程序502使用连接验证结果和告警信息来显示640和突出显示被告警影响的第2层（506）和第3层（504）对象。连接验证结果可以与642交互以产生与特定连接验证任务和/或连接验证测试有关的第2层和第3层对象的显示640。

参考图7，根据本发明典型实施例的使用情况，操作管理人员可以容易地验证显示在网络图中的 VPN 连接。根据该实例，只提供两个 VPN1和2。该操作管理人员通过分别选择 VPN1和 VPN2来定义两个连接验证任务 J1和 J2。选择 VPN1和 VPN2，分别规定在路由器（102）R1，R2和 R3接口之间执行的连接验证测试 T1，T2，T3，T4，T5和 T6 ，并且进一步规定在路由器（102）R2和 R4之间执行的连接验证测试 T7和 T8。在选择两个连接验证任务 J1和 J2之后，通过单击，操作管理人员调度610连接验证任务以立即执行。

根据本发明典型实施例的典型实现方案，图8显示了使得操作管理人员能够在网络管理环境中集中地处理连接验证任务的典型的用户接口。

在处理关于两种类型的连接验证测试——ping和traceroute的定义的(604)连接验证任务中使用连接验证任务处理窗口800。

连接验证任务处理窗口800包含三个区域：一个连接验证任务窗格802，一个结果窗格，和一个统计量窗格806。连接验证任务窗格802包含连接验证任务列表，连接验证任务在该列表中已经定义604和/或保存612并准备用于调度。

下表1描述了在连接验证任务列表802中典型的连接验证任务字段项：

栏目	描述
类型	连接验证任务类型，ping 还是 traceroute
名称（未示出）	与连接验证任务相关的名称
源	从中执行连接验证测试的源被管理实体
目的地	相应的目的地被管理实体
超时（ms）	用来等待来自目的地的测试响应的超时
数量	在任务中单个测试的数量
间隔（sec）	在发送的 ICMP 分组之间的间隔
状态	连接验证任务的状态

表1：典型的连接验证任务字段项

下表2描述了典型的连接验证任务状态，相应的连接验证任务状态图900显示在图9中：

连接验证任务状态
启动－连接验证任务刚被建立/未被调度
处理中－连接验证任务被调度，还没有获得结果
已完成－连接验证任务结果已被接收
已取消－连接验证任务已取消，结果不可得到
错误－关于连接验证任务的错误已经发生
通信错误－发生了通信错误，任务取消

表2：典型的连接验证任务状态

基于连接验证任务的状态，只有某些动作是可获得的。只有当连接验证任务第一次加到连接验证任务列表802(或从文件中检索出)时发生连接验证任务的“启动”状态。一旦被调度610，连接验证任务将停留在“处理中”状态，直到操作管理人员取消该连接验证任务，或者连接验证任务完成。当操作进入“已完成”或者“已取消”状态时，操作管理人员可以调度连接验证任务或者从连接验证任务列表802中删除该连接验证任务。在服务器故障期间“通信错误”状态实际上就充当“已取消”状态。如果对于相同的源被管理实体多个连接验证任务被排队，等待连接验证任务状态将是“处理中”，虽然当前运行/排队的连接验证任务完成。

连接验证任务列表802包含产生的所有定义的 ping 和 traceroute 连接验证任务并且可由“类型”栏区分。

图10和图11显示了窗口1000和1100，其使得能够分别定义连接验证 ping 和 traceroute 任务。下表3详细描述了为每个单独的 ping 连接验证任务规定的典型参数:

字段	描述
名称（未示出）	ping 连接验证任务的名称
源	源被管理实体，在其上执行连接验证任务
目的地	目的地被管理实体
ping 的次数	ping 探测分组发送的次数
间隔（秒）	在 ping 探测之间等待的时间
分组大小（字节）	ping 探测分组大小
填充模式	给 ping 探测分组填充的值
每个 ping 的超时（毫秒）	等待响应的超时期间
业务类型	业务类型（或 DSCP 位）

表3: 典型的 ping 连接验证任务参数

下表4详细描述了为每个单独的 traceroute 连接验证任务规定的典型参数:

条目	描述
名称	traceroute 连接验证任务的名称
源	源被管理实体，在其上执行连接验证任务
目的地	目的地被管理实体
最大 TTL	最大生存时间
每跳探测	发送给路由中的每个跳的 ping 探测数量
间隔（秒）	在发出下一个 traceroute 之前的等待期间
分组大小（字节）	ICMP 分组大小
填充模式	给 ICMP 分组填充的值
每个探测的超时（毫秒）	等待响应的超时期间
UDP 端口	将 traceroute 发送到的端口

表4：典型的 traceroute 连接验证任务参数

ping 和 traceroute 连接验证任务具有相同有效的源和目的地被管理实体。为规定路由器、节点或 LSP，用户可以如上所述地选择它600。

源 NMS 被管理实体包括，但本发明不限于：路由器（由 NMS 管理的路由器），第一跳 LSP（确定源路由器），VPN（VRF 名称）等。如果选择 LSP，路由器和 IP 地址字段用包括源路由器的管理 IP 地址的、来自 LSP 的源端点的信息进行填充。

目的地 NMS 被管理实体包括，但本发明不限于：任何 IP 地址（NMS 管理的路由器和未管理的路由器），路由器，路由器接口（编号的和未编号的（路由器 ID－串）），LSP（被确定为 LSP 的目的地端点的目的地路由器）等。为了规定不被 NMS 管理的目的地通信网络实体，操作管理人员必须规定目的地实体的 IP 地址。如果选择了 LSP，用来自 LSP 的目的地端点的信息填充路由器和 IP 地址字段。

选择接口，源路由器或节点的相关 IP 地址被填充。如果 VRF 名称与所选择的路由器接口相关，那么将用它来自动填充 VRF 名称。

规定路由器或节点的另一方法是基于管理 IP 地址查询容器层次体系508。操作管理人员可以将 IP 地址填充到 IP 地址字段中，然后按“回车”按键。如果这是所支持的路由器或节点的管理 IP 地址，则它的详细资料被填充。

为连接验证任务定义的所有参数适用于基于该连接验证任务执行的所有连

接验证测试。

一旦源、目的地和相应参数被规定，通过点击“添加”按钮则将连接验证任务添加到连接验证任务列表802中，连接验证任务列表802可以被保存到文件或者储存库512以便以后检索，该检索使得能够重新使用定义604的连接验证任务。

返回到图8，添加到操作列表中的连接验证任务不能自动地开始 ping 或 traceroute 操作，其必须通过选择配置验证任务、右点击、从弹出菜单中选择“启动”来调度610。通过相同的弹出菜单，配置验证任务可以被取消或删除。

选择多个连接验证任务使得操作管理人员能够通过单击按键810一次调度610多个连接验证任务。

为了观察连接验证任务的结果，连接验证任务必须“已完成”。当从连接验证任务列表802中选择了已完成的连接验证任务时，结果窗格806被更新。如果所选择的连接验证任务在处理中，那么结果窗格806是消隐状态并且当接收到632结果时自动进行更新。

结果窗格804显示来自完成的 ping 或 traceroute 连接验证测试的接收632结果，包括来自每个单独的 ping 或 traceroute 连接验证测试的所产生的成功状态、和延时。当显示关于 traceroute 连接验证任务的结果时，结果窗格804还显示跳信息，如图12所示。

根据本发明的典型实施例，操作管理人员具有规定该连接验证被周期执行的手段。

图13显示了使得操作管理人员能够为连接验证任务定义606进度表的典型窗口1300。表5详述了典型的连接验证任务安排进度参数：

条目	描述
处理间隔	进度表的每次运行之间的时间
频率	连接验证任务的频率
开始日期	该进度表开始运行的日期
开始时间	该进度表开始运行的时间
结束日期	该进度表结束运行的日期
结束时间	该进度表结束运行的时间

表5：典型的连接验证任务安排进度参数

如果没有规定时间帧，该处理间隔字段标识在该进度表自身每次运行之间的时间。如果规定频率为0，在规定的开始日期/时间调度该连接验证任务一次，该结束日期/时间被忽视。

连接验证进度表可以进行列表，表6显示了用于进度列表项的典型字段：

栏目	描述
启用	其是启用或禁止每个进度运行的校验框
进度	进度的唯一名称
开始时间	进度的开始时间
结束时间	进度的结束时间
频率	在连接验证任务之间的时间
频率周期	频率的类型（例如天，小时，分等）
告警状态	识别还未确认的最高严重程度告警
状态	进度状态，从最高连接验证任务状态中得到

表6：典型的进度列表项字段

进度列表包含定义的606进度，该进度通过它唯一的名称来识别每个进度。通过点击包含在与进度相关的“启动”字段中的校验框来允许启用/禁止该进度。

当连接验证测试必须在相同的源管理实体上执行时，只需要被访问的进度可以重叠。如果多个进度重叠，来自一个进度的连接验证测试可以和来自另一个进度的连接验证测试交替。如果一个进度不能在规定的频率内完成，下一个重复将被跳过。

在连接验证任务完成后返回到图8/图12，操作管理人员可以选择完成的连接验证任务和在结果窗格804中显示结果。下表7详细描述了关于完成的连接验证测试的典型结果项字段：

栏目	描述
IP地址/跳	ping 探测分组的目的地 IP 地址，或者用于 traceroute 的跳的 IP 地址
序列	单独 ping 或跳的序列号
延时（毫秒）	来自目的地的响应的延时

表7：典型的完成的连接验证测试结果项字段

如果一个 ping 探测分组遇到了错误（即，有效的诊断错误例如网络不能达到或者节点不能达到），用于该单独项的延时栏目将显示该错误。

图14显示了使得操作管理人员能够为连接验证任务定义至少一个阈值520的典型窗口1400。表8详细描述了典型的连接验证任务阈值参数：

阈值	条目	值	描述
N/A	总期间	5-1440	在计算总的统计量之前重复的次数
抖动（毫秒）	值	0-60000	在发出抖动告警之前以毫秒表示的最大变化。特定的告警严重性可以和该阈值关联。
	严重性	临界的 主要的 次要的 警告的	
	（校验框）	禁止 启用	启用或禁止该阈值
延时（毫秒）	值	0-60000	在发出往返延时告警之前以毫秒表示的最大延时。特定告警严重性可以和该阈值关联。
	严重性	临界的 主要的 次要的 警告的	
	（校验框）	禁止 启用	启用或禁止该阈值
分组丢失(%)	值	0-100	在发出连接告警之前允许的连接故障的次数。特定的告警严重性可以和该阈值关联。
	严重性	临界的 主要的 次要的 警告的	
	（校验框）	禁止 启用	启用或禁止该阈值

表8：典型的连接验证任务阈值参数

总期间字段识别在计算总的统计量之前的重复等待次数，并且发出告警。如果该重复被跳过，那么该重复将不包含在总期间内。该阈值字段识别阈值限和如果发出告警时使用的相关的告警严重性。当没有满足数据分组流需求时，为期望的连接验证测试结果设置阈值来触发告警，提供确保遵守 SLA 协议的监视手段。表

9详细描述了根据规定的阈值产生的典型告警级别:

描述
临界的告警-产生临界的告警
主要的告警-产生主要的告警
次要的告警-产生次要的告警
警告的告警-产生警告的告警
错误-在总期间内发生的错误
正常-没有错误或告警

表9: 用于在操作列表中的每个操作的状态值

返回到图8/图12，统计窗格806显示关于连接验证任务的统计量，例如抖动和分组丢失百分比。在 traceroute 连接验证任务的情况下，统计量是基于在结果窗格804中选择的跳。

结果和统计量可以两种格式——文本或者 CSV 中的一种存到本地文件中。以下是典型的文本格式文件:

Ping New York-Boston

源 138.120.15.90: vrf-VPN1 目的地 13.13.13.2

序列号	源	目的地	延时(毫秒)
1	138.120.15.90	13.13.13.2	112
2	138.120.15.90	13.13.13.2	节点不能到达
3	138.120.15.90	13.13.13.2	98

%丢失: 0.0 抖动(毫秒): 0.0最小/最大/平均(毫秒): 1.0/1.0/1.0

traceroute New York- Boston

源 138.120.15.90: vrf-VPN1目的地 56.56.56.56

序列号	目的地	延时(毫秒)
1	12.12.12.1	10,节点不能到达,5
2	13.13.13.2	4,6,6

以下是典型的相应 CSV 格式文件:

Ping ,New York- Boston

源,138.120.15.90:vrf-VPN1,目的地,13.13.13.2

序列号,源,目的地,延时(毫秒)

1 ,138.120.15.90,13.13.13.2,112

2 ,138.120.15.90,13.13.13.2,节点不能到达

3 ,138.120.15.90,13.13.13.2,98

%丢失(毫秒),0.0

抖动(毫秒),0.0

最小(毫秒),1.0

最大(毫秒),1.0

平均(毫秒),1.0

traceroute,New York- Boston

源,138.120.15.90:vrf-VPN1,目的地13.13.13.2

序列号,目的地,延时(毫秒)

1 ,12.12.12.1,10,节点不能到达,5

2 ,13.13.13.2,4,6,6

历史的结果可以存储在包含每个执行的ping和traceroute连接验证任务的结果的储存库512中。

因此,根据本发明的典型实施例,对在使用NMS系统的网络管理环境中的服务提供商IP/MPLS通信网络中的连接进行验证是通过以下解决的:

-在规定的源和目的地被管理实体之间,执行直接的ping和traceroute连接验证测试;

-在路由器和IP接口之间执行连接验证测试;

-通过MPLS LSP执行连接验证测试;

-在VPN(VPN路由和转发(VRF)-VLAN ID标记的VPN。见在此引入作为参考的RFC 2547 L3VPN)中执行连接验证测试;

-在选择的被管理实体和未被管理的实体,例如但不限于路由器之间执行连接验证测试;对于未被管理的实体的网络寻址被发现;

-对多个测试安排进度以周期地验证连接;

-安排多个测试来获得分组业务统计量（延时，抖动，丢失）；

-在多个连接验证测试进度结果上配置告警阈值，以便确保满足服务等级协议（SLA）；和

-突出显示在NMS系统504/506上显示的640失败的或成功的分组传输路由。

总之，连接验证结构500使得操作管理人员能够与在集中网络管理环境中的NMS系统510上执行的连接验证应用程序502交互，以收集来自被管理的通信网络的实时连接信息用于维护和诊断。

所提出的解决方案带来的优点包括:

-在网络管理系统中执行的简单的解决方案，因为提供连接验证测试被集中并且不需要人工登录特定的源被管理实体。

-该解决方案提供要被周期性执行的连接验证测试进度表，其节省操作管理人员的时间，因此减少服务提供商的运营成本。

-该解决方案通过提供即时告警和为后面分析而总结的结果来增加IP连接的可靠性，可用性，可服务性。

-为了解决服务提供商网络问题，该解决方案提高并简化该IP诊断和维护能力。其而且在启用数据业务之前允许测试网络提供。

-因为管理通过与NMS系统相关的GUI执行，与在逐个源网络节点（路由器）基础上使用传统CLI相比，该配置容易得多，传统CLI是易于出错的。

-更多优点包括能观察/配置/修改/存储多个网络连接验证测试，并在网络管理环境中提供即时的（通过查看和告警）或历史的结果信息。

-减少操作开支对服务提供商是重要的。本发明使创建和维护连接测试的诊断过程自动化，由此减少执行维护和诊断功能的操作成本，该维护和诊断功能确保IP连接满足用户对抖动、延时和数据丢失的期望。此外，减少操作成本并且增加可靠性，这两者对服务提供商都是有价值的。

给出的实施例只是示例性的，对于本领域技术人员来说，应该理解在不脱离本发明精神的前提下，对上述实施例可进行改变。本发明的保护范围仅由所附的权利要求书定义。

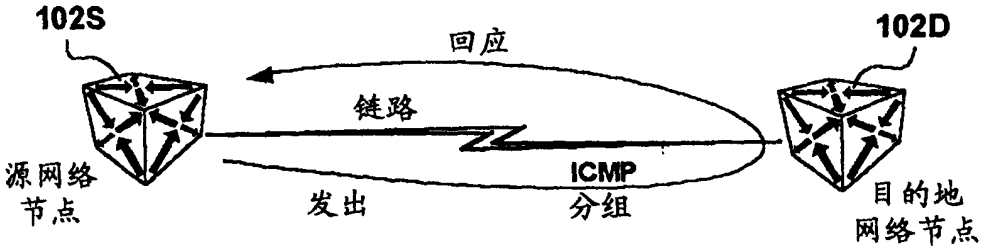


图 1
现有技术

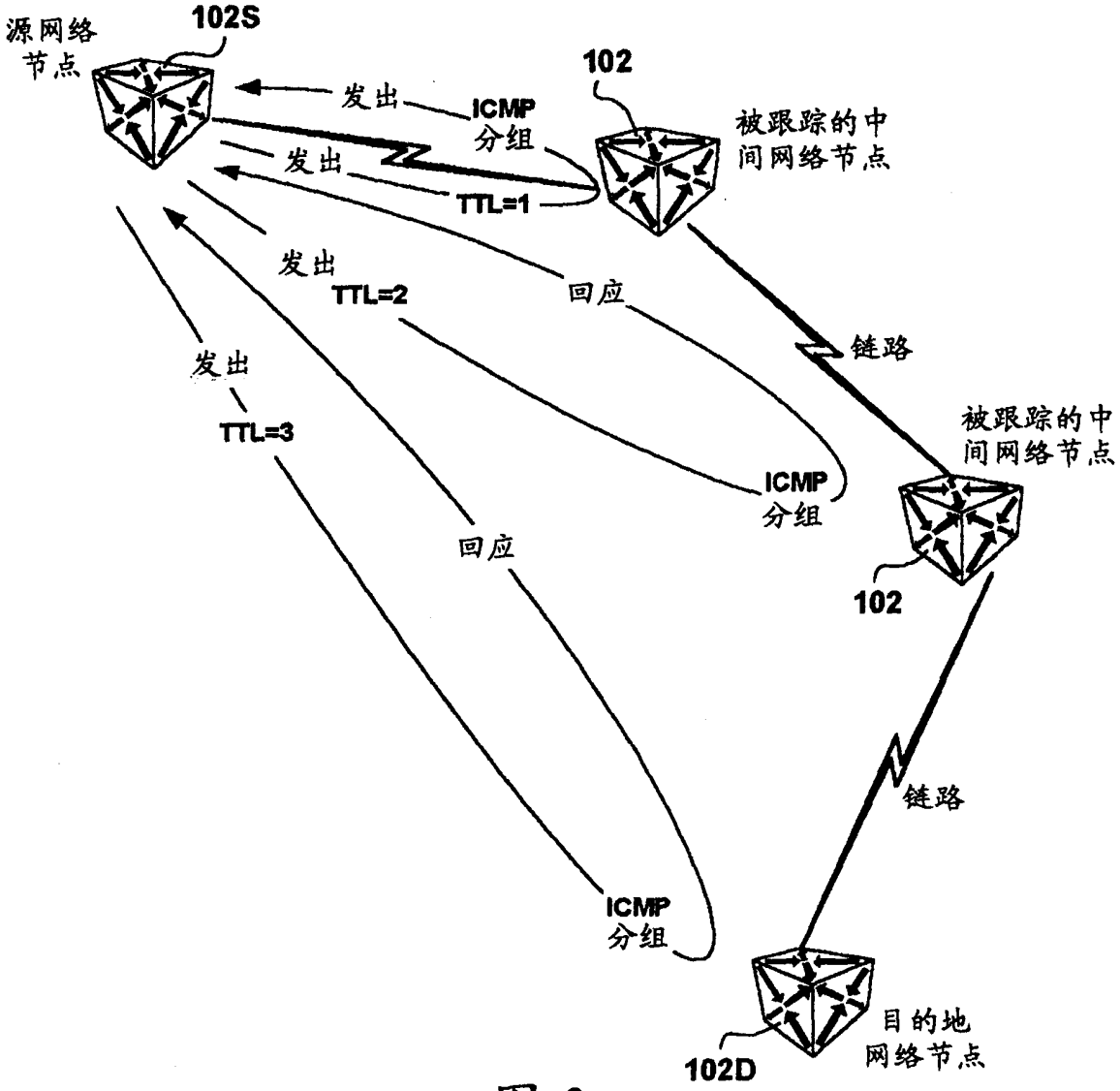


图 2
现有技术

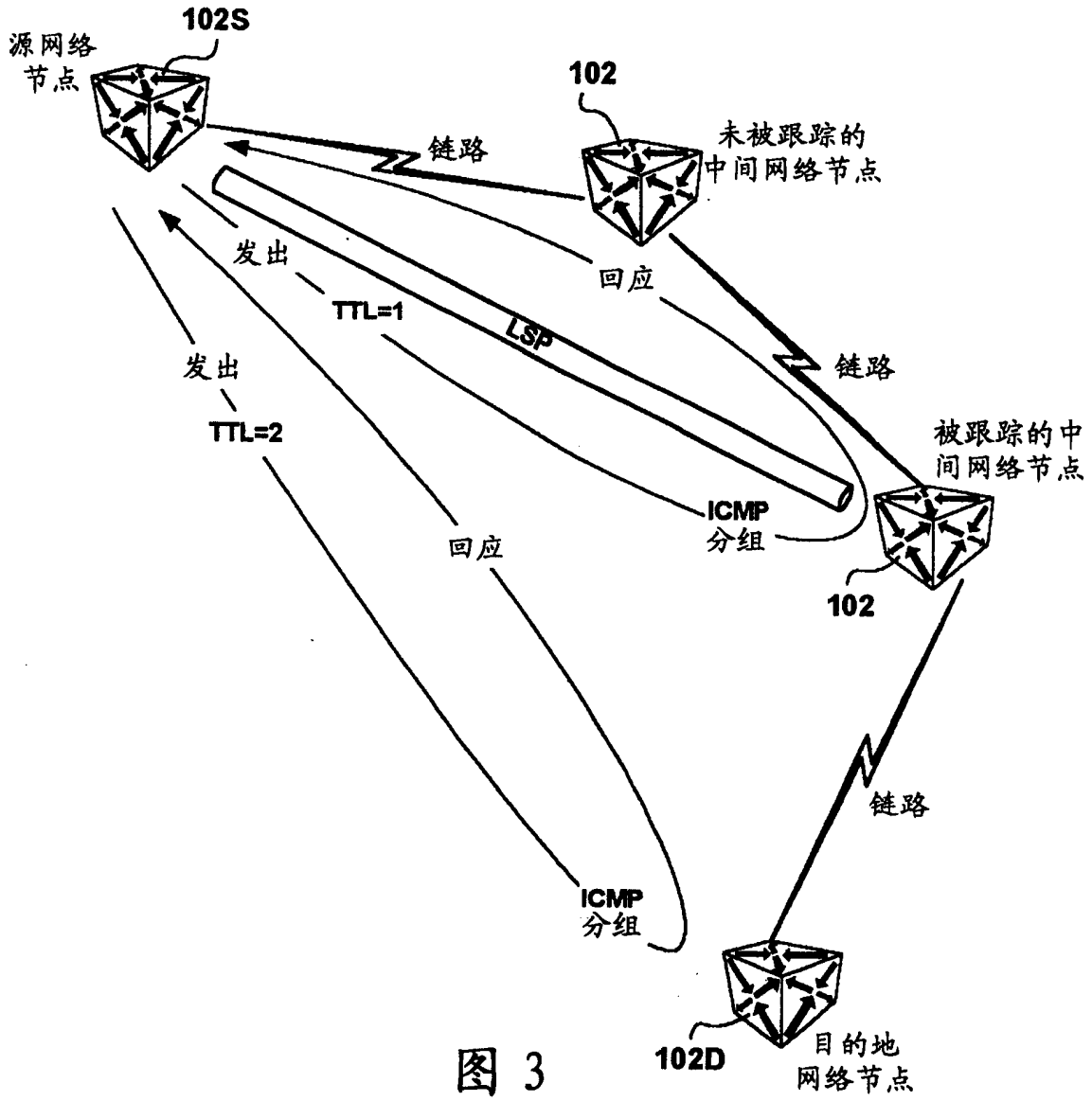

102S
源网络
节点
102
未被跟踪的
中间网络节点
链路
发出
TTL=1
LSP
回应
链路
发出
TTL=2
被跟踪的中
间网络节点
ICMP
分组
回应
102
链路
ICMP
分组
102D
目的地
网络节点

图 3
现有技术

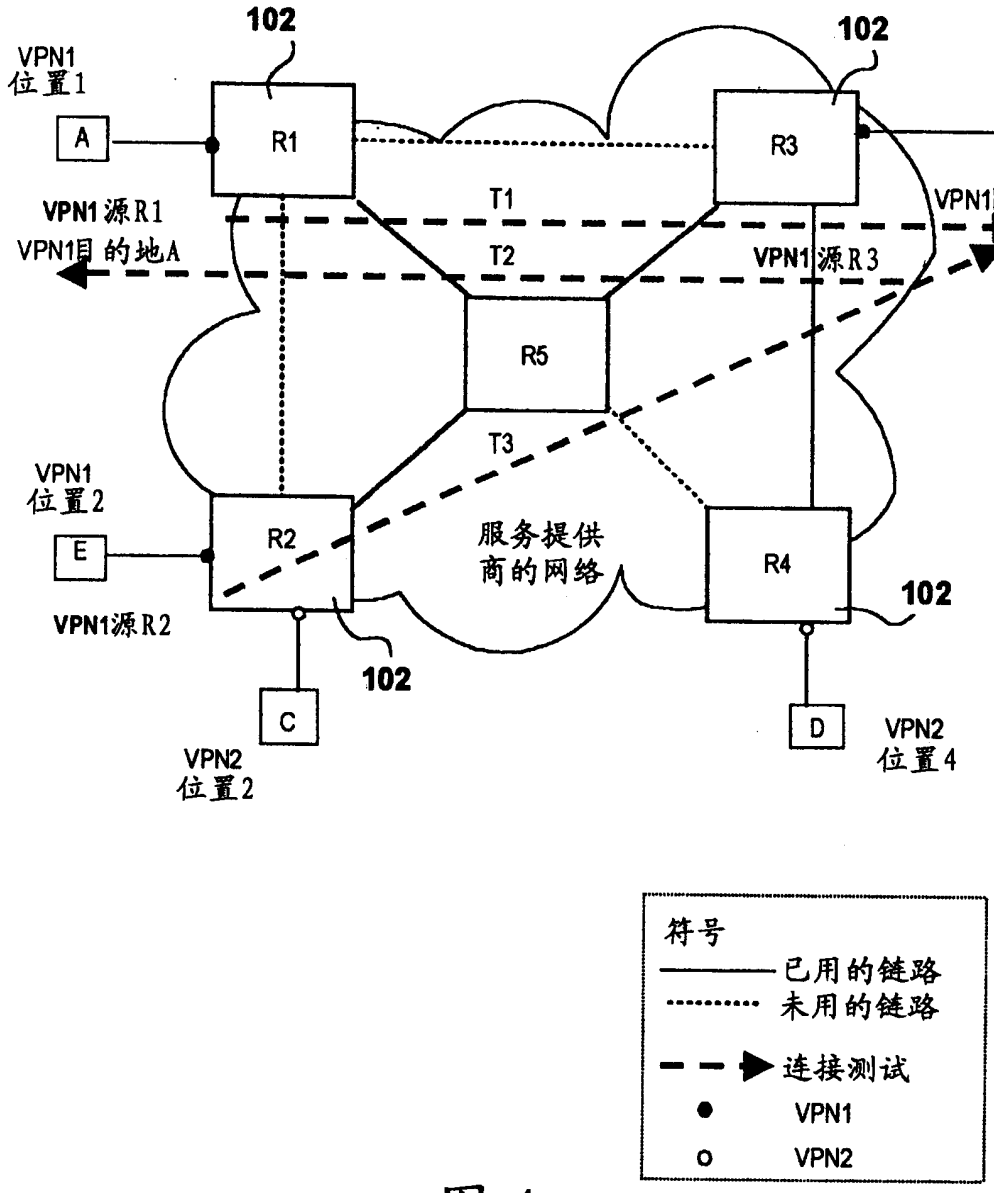

102
102
VPN1
位置1
VPN1
位置3
A
R1
R3
B
T1
VPN1源R1
VPN1目的地A
VPN1目的地B
T2
VPN1源R3
R5
T3
VPN1
位置2
E
R2
服务提供
商的网络
R4
102
VPN1源R2
102
C
D
VPN2
位置4
VPN2
位置2
符号
已用的链路
未用的链路
连接测试
VPN1
VPN2

图 4
现有技术

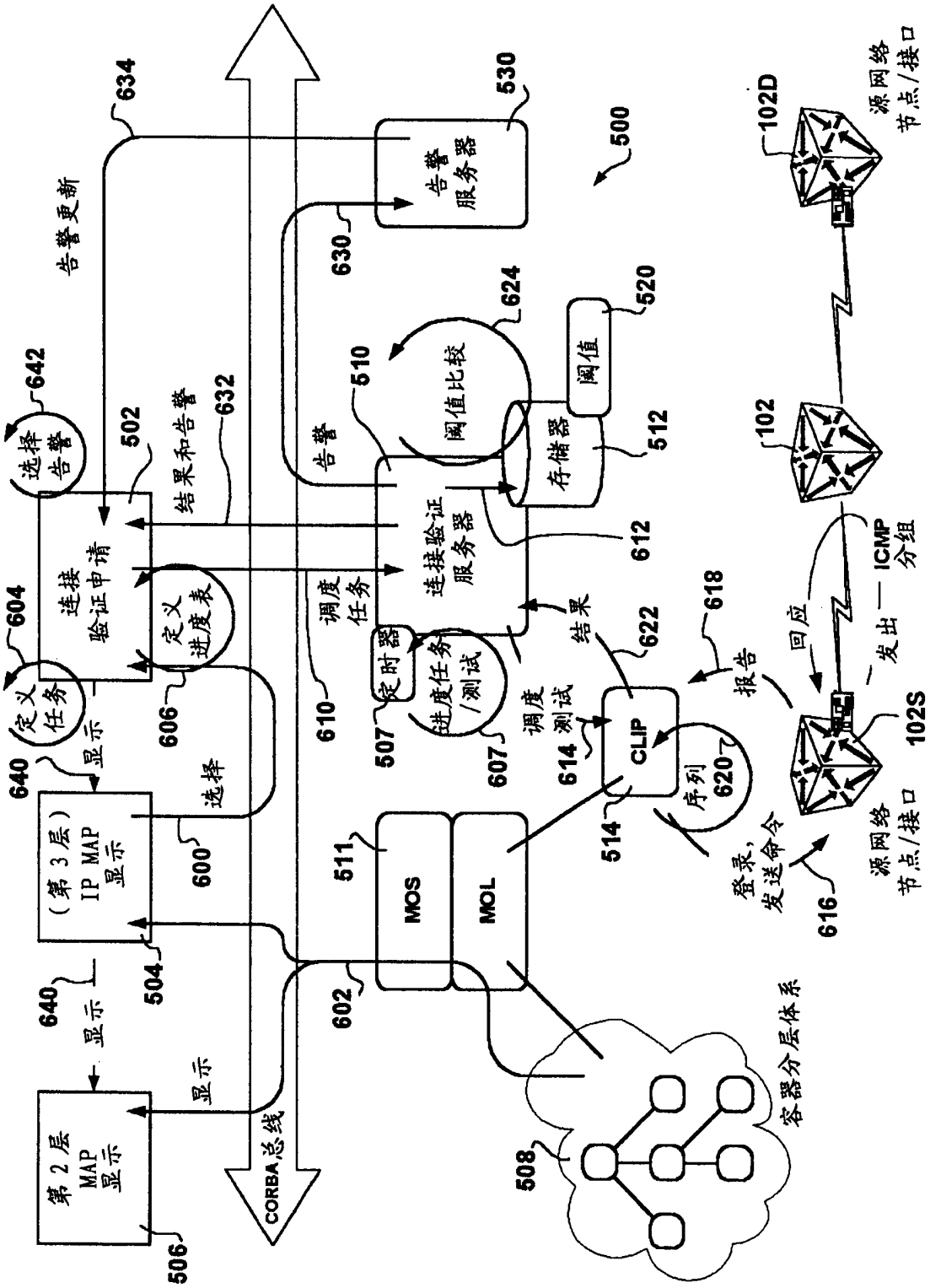

500
CORBA总线
第2层 MAP 显示
506
(第3层) IP MAP 显示
504
显示
640
显示
640
定义任务
640
选择告警
642
连接验证申请
604
定义进度表
606
选择
600
告警更新
634
结果和告警
632
502
告警
510
调度任务
610
定时器
507
进度任务/测试
607
连接验证服务器
612
阈值比较
624
存储器
512
阈值
520
告警服务器
530
630
结果
622
调度测试
614
CLIP
514
序列
620
报告
618
MOS
511
MOL
602
容器分层体系
508
登录,发送命令
616
回应
发出 — ICMP 分组
源网络节点/接口
102S
102
102D
源网络节点/接口

图 5

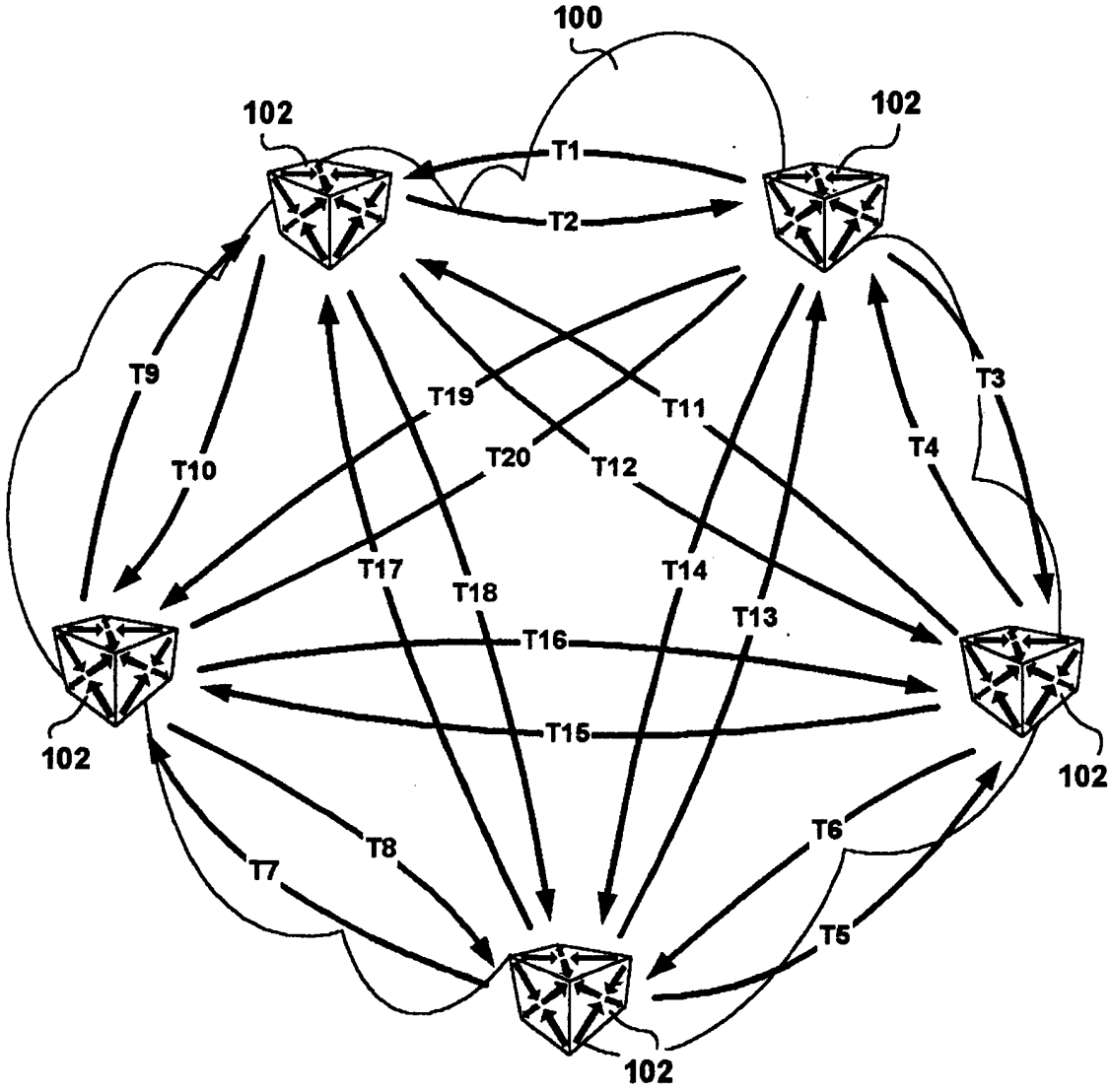

100
102
102
T1
T2
T3
T4
T5
T6
T7
T8
T9
T10
T11
T12
T13
T14
T15
T16
T17
T18
T19
T20
102
102
102

图 6

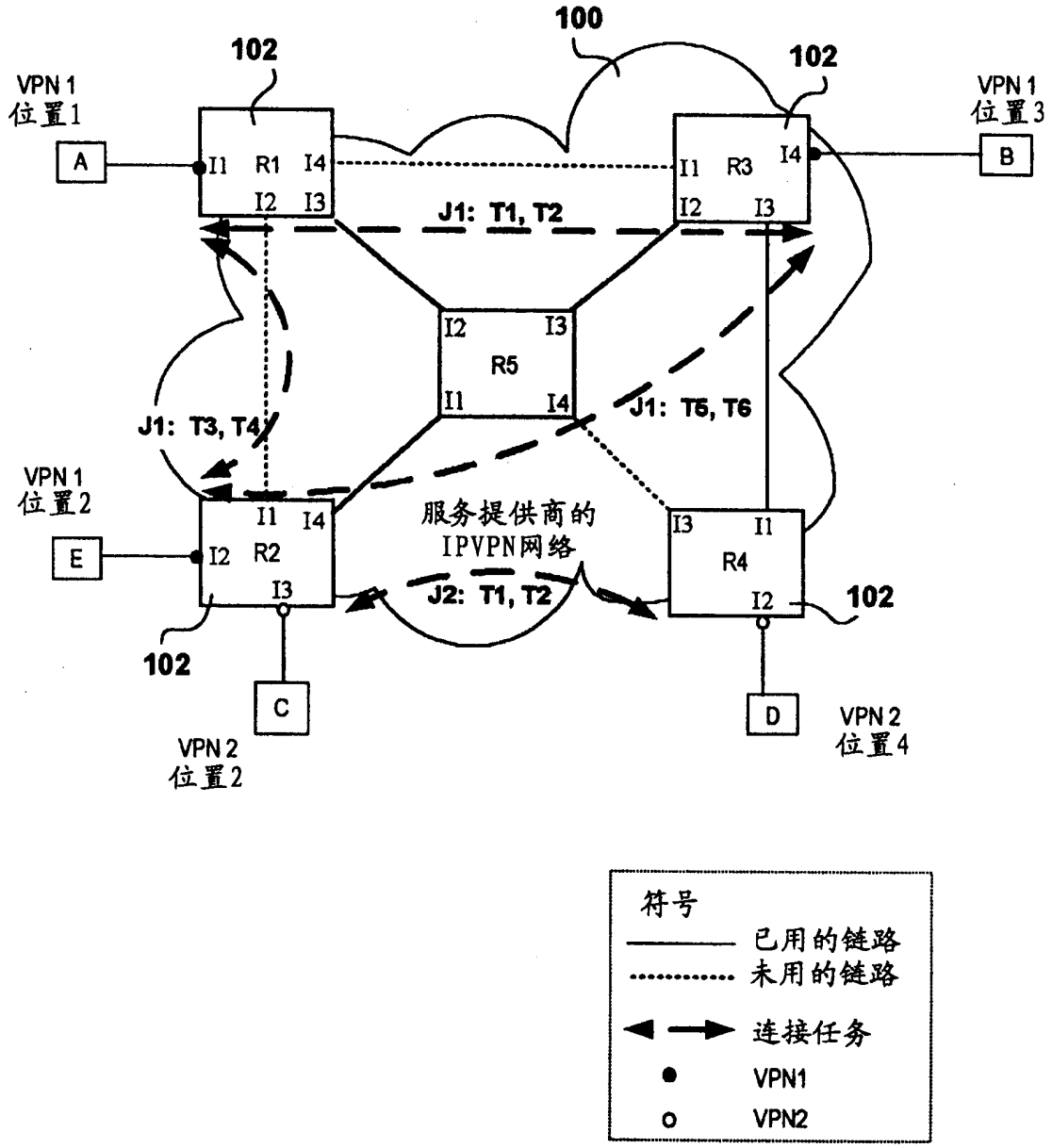

100
102
102
VPN 1
位置1
VPN 1
位置3
A
B
I1 R1 I4
I2 I3
I1 R3 I4
I2 I3
J1: T1, T2
I2 I3
R5
I1 I4
J1: T3, T4
J1: T5, T6
VPN 1
位置2
E
I1 I4
I2 R2
I3
服务提供商的
IPVPN网络
J2: T1, T2
I3 I1
R4
I2
102
102
C
D
VPN 2
位置2
VPN 2
位置4
符号
已用的链路
未用的链路
连接任务
VPN1
VPN2

图 7

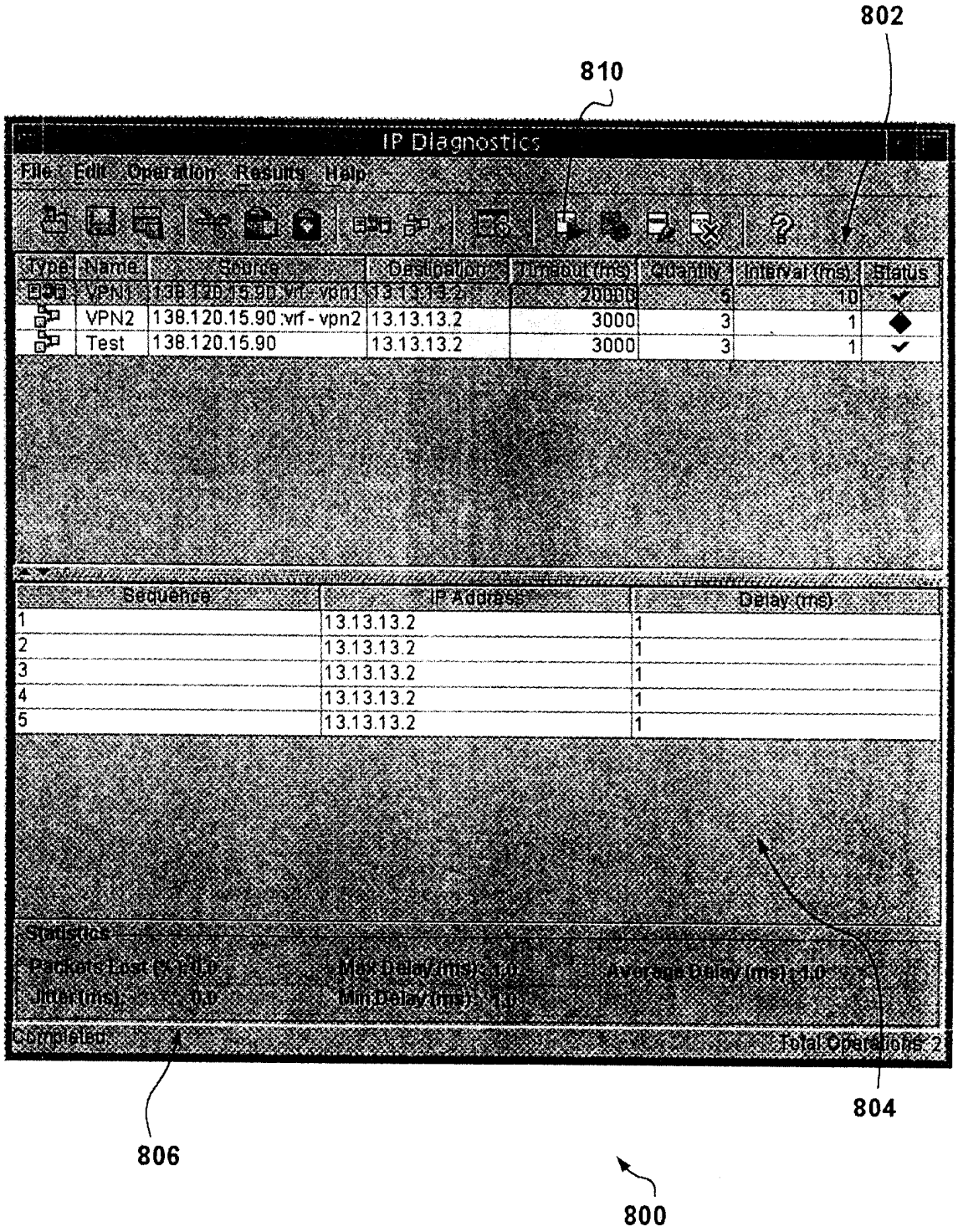

802
810
IP Diagnostics
File Edit Operation Results Help
Type Name Source Destination Timeout (ms) Quantity Interval (ms) Status
VPN1 138.120.15.90 :vrf - vpn1 13.13.13.2 20000 5 10
VPN2 138.120.15.90 :vrf - vpn2 13.13.13.2 3000 3 1
Test 138.120.15.90 13.13.13.2 3000 3 1
Sequence IP Address Delay (ms)
1 13.13.13.2 1
2 13.13.13.2 1
3 13.13.13.2 1
4 13.13.13.2 1
5 13.13.13.2 1
Statistics
Packets Lost (%) 0.0
Jitter (ms) 0.0
Max Delay (ms) 1.0
Min Delay (ms) 1.0
Average Delay (ms) 1.0
Completed
Total Operations 2
804
806
800

图 8

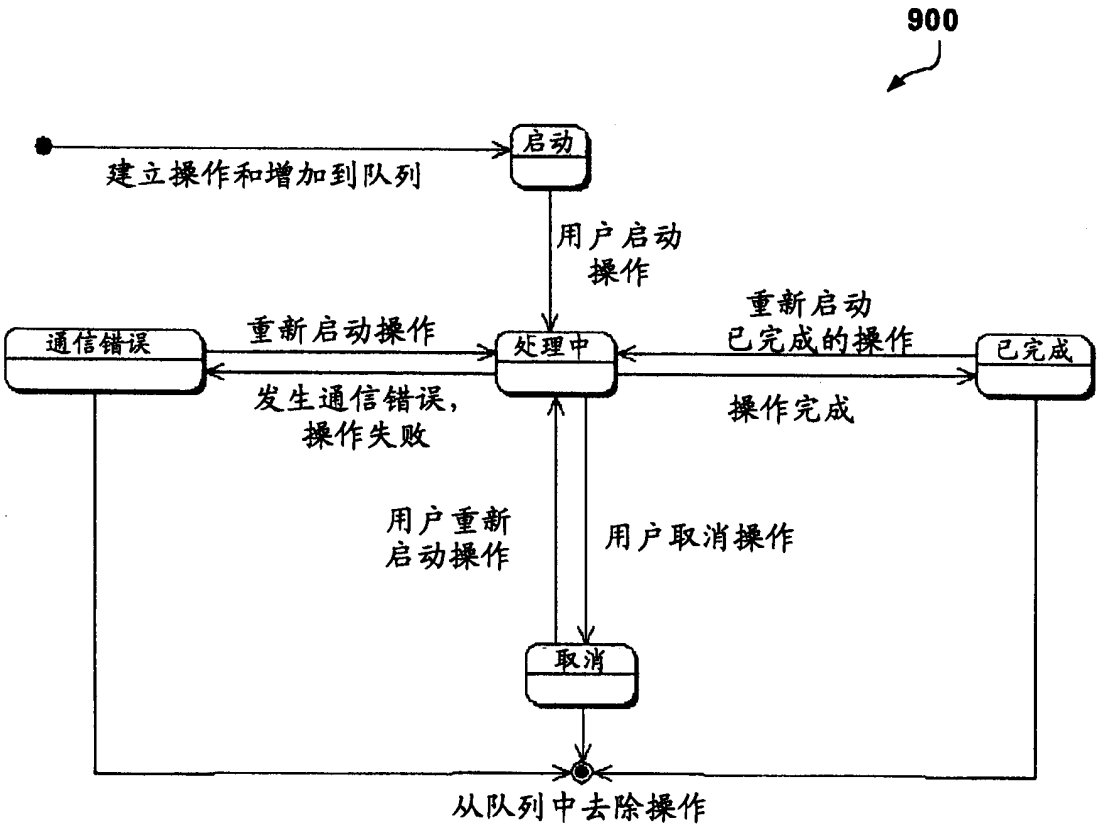

900
启动
建立操作和增加到队列
用户启动
操作
通信错误
重新启动操作
处理中
重新启动
已完成的操作
已完成
发生通信错误，
操作失败
操作完成
用户重新
启动操作
用户取消操作
取消
从队列中去除操作

图 9

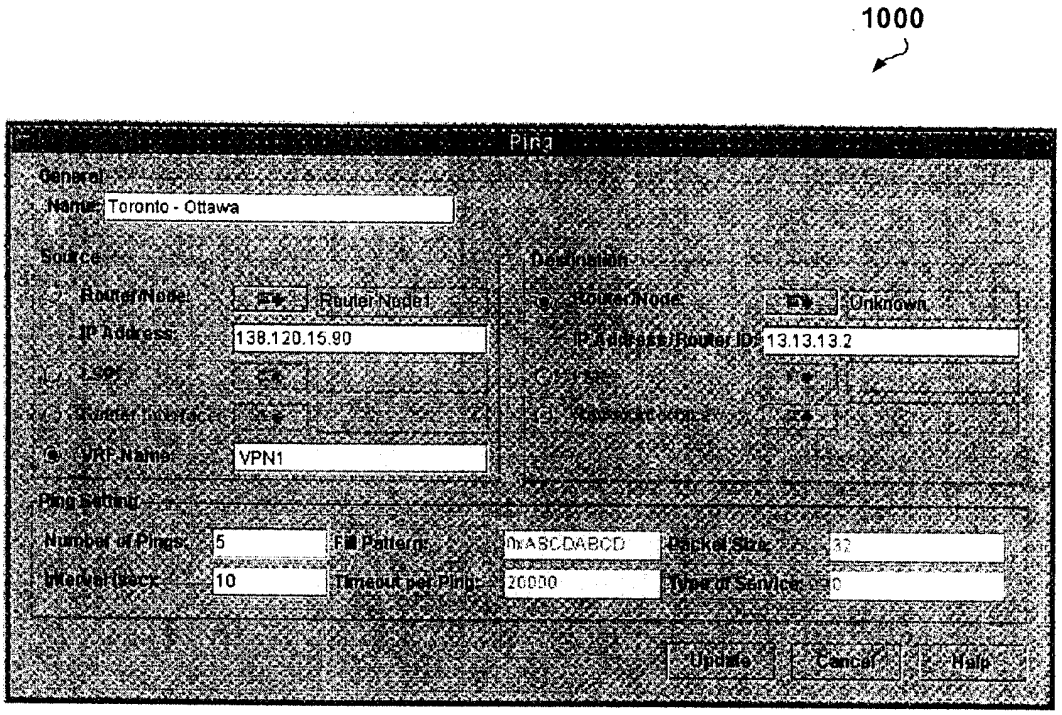

1000
Ping
General
Name: Toronto - Ottawa
Source
Router Node:
Router Node1
IP Address:
138.120.15.90
VRF Name:
VPN1
Destination
Router Node:
Unknown
IP Address/Router ID:
13.13.13.2
Ping Setting
Number of Pings:
5
Fill Pattern:
0xABCDABCD
Packet Size:
32
Wait Interval:
10
Timeout per Ping:
20000
Type of Service:
0
Update
Cancel
Help

图 10

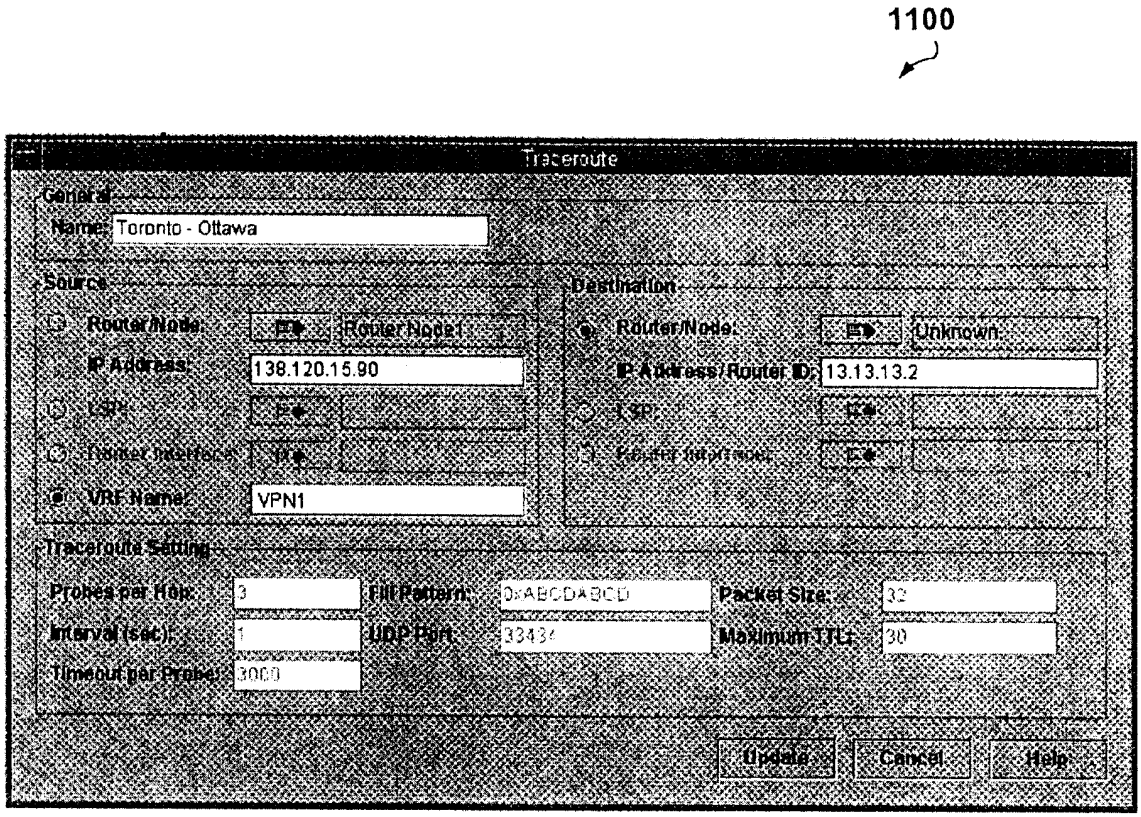

1100
Traceroute
General
Name: Toronto - Ottawa
Source
Router Node:
Router Node1
IP Address:
138.120.15.90
VRF Name:
VPN1
Destination
Router Node:
Unknown
IP Address/Router ID:
13.13.13.2
Traceroute Setting
Probes per Hop:
3
Interval (sec):
1
Timeout per Probe:
3000
Fill Pattern:
0xABCDABCD
UDP Port:
33434
Packet Size:
32
Maximum TTL:
30
Update
Cancel
Help

图 11

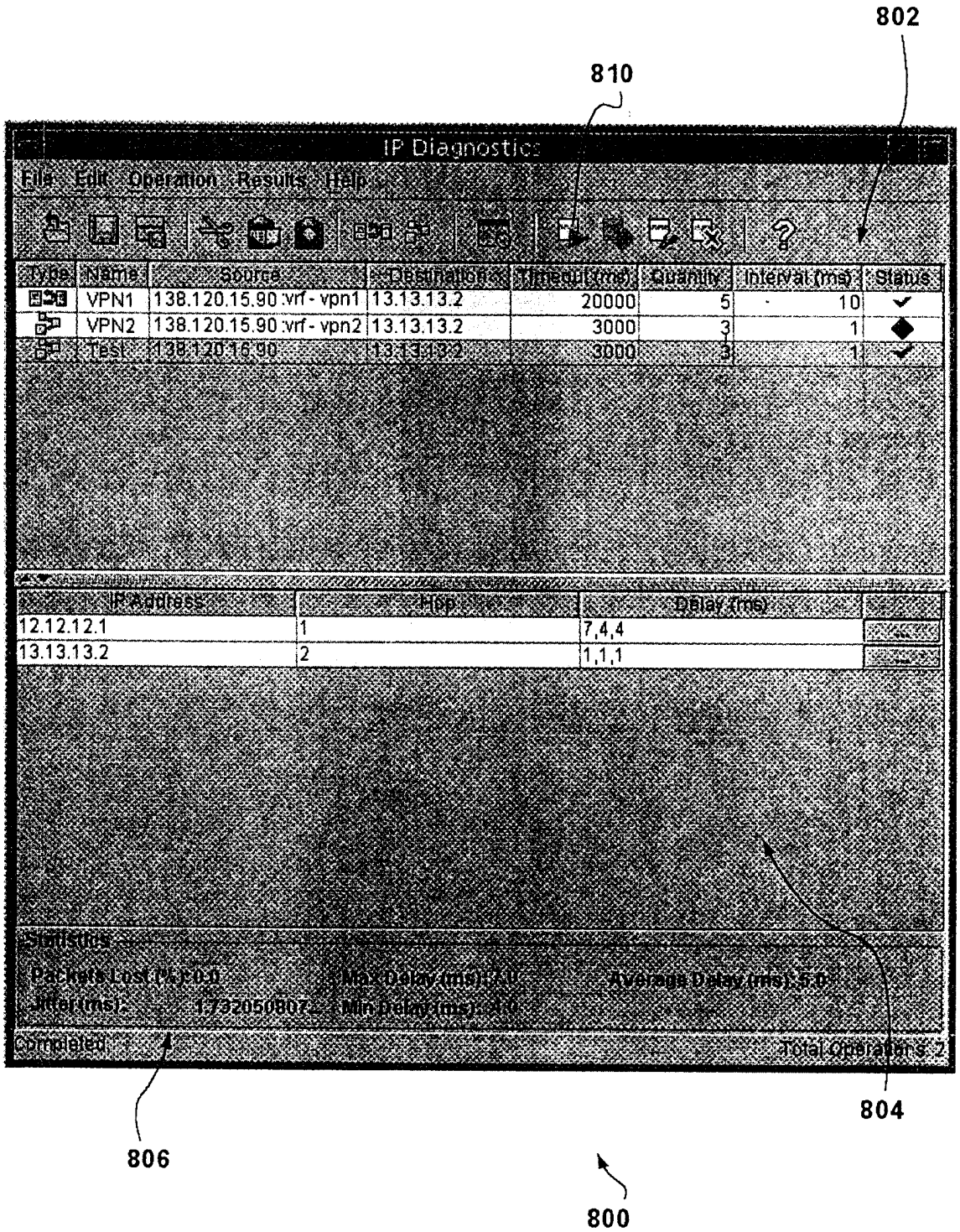

802
810
IP Diagnostics
File Edit Operation Results Help
Type Name Source Destination Timeout (ms) Quantity Interval (ms) Status
VPN1 138.120.15.90 :vrf - vpn1 13.13.13.2 20000 5 10
VPN2 138.120.15.90 :vrf - vpn2 13.13.13.2 3000 3 1
Test 138.120.16.90 13.13.13.2 3000 3 1
IP Address Hop Delay (ms)
12.12.12.1 1 7,4,4
13.13.13.2 2 1,1,1
Statistics
Packets Lost (%) 0.0
Max Delay (ms): 7.0
Average Delay (ms): 5.0
Jitter (ms): 1732050807
Min Delay (ms): 4.0
Completed
Total Operations: 2
804
806
800

图 12

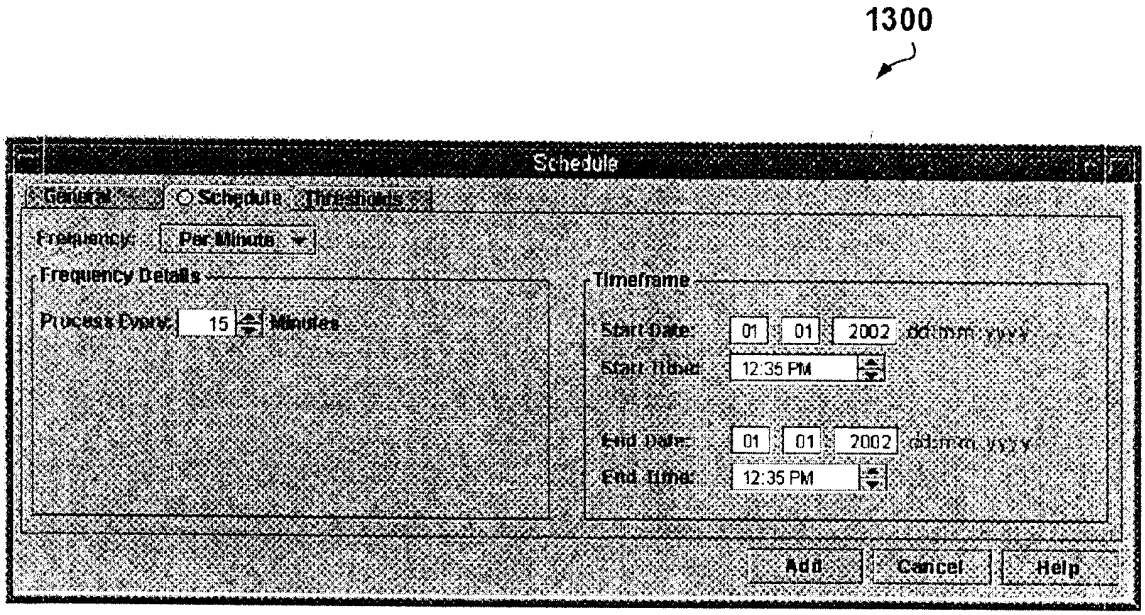

1300
Schedule
General
Schedule
Thresholds
Frequency:
Per Minute
Frequency Details
Process Every:
15
Minutes
Timeframe
Start Date:
01
01
2002
dd:mm:yyyy
Start Time:
12:35 PM
End Date:
01
01
2002
dd:mm:yyyy
End Time:
12:35 PM
Add
Cancel
Help

图 13

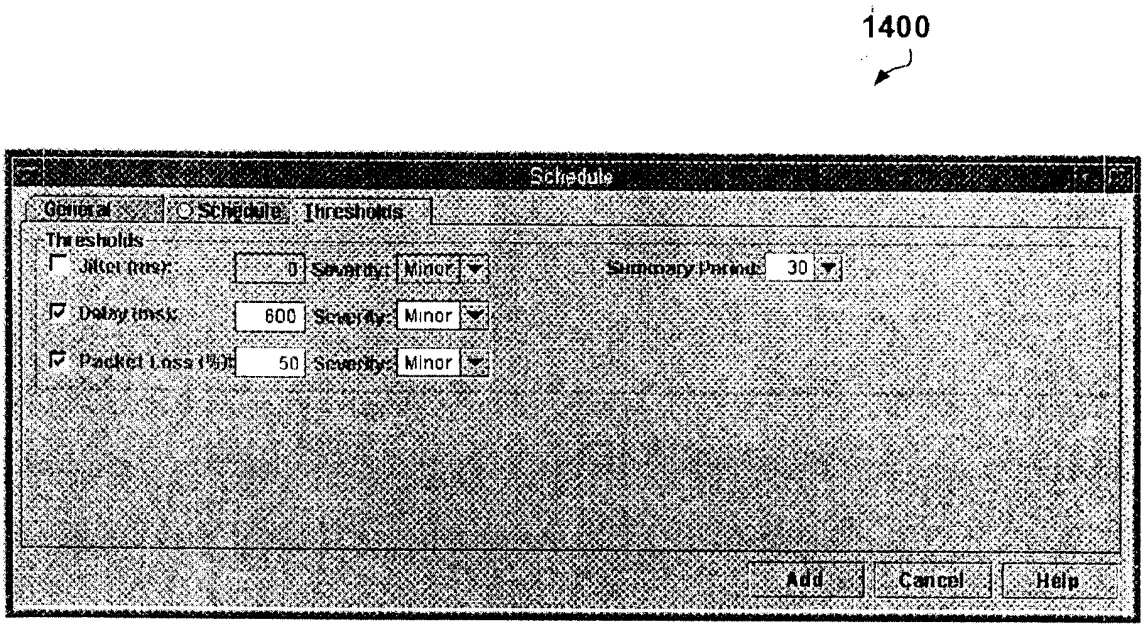

1400
Schedule
General
Schedule
Thresholds
Thresholds
Jitter (ms):
0
Severity:
Minor
Summary Period:
30
Delay (ms):
600
Severity:
Minor
Packet Loss (%):
50
Severity:
Minor
Add
Cancel
Help

图 14