(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 101622834 B
(45)授权公告日 2013.03.13

(21)申请号 200880006626.6
(22)申请日 2008.02.21
(30)优先权数据
11/712,123 2007.02.28 US
(85)PCT申请进入国家阶段日
2009.08.28
(86)PCT申请的申请数据
PCT/US2008/054485 2008.02.21
(87)PCT申请的公布数据
WO2008/106355 EN 2008.09.04
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 S·赫佐格 M·哈格曼
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 顾嘉运 钱静芳
(51)Int.Cl.
H04L 29/08(2006.01)
(56)对比文件
CN 1558606 A,2004.12.29, 全文.
US 20060029083 A1,2006.02.09, 全文.
US 20020118644 A1,2002.08.29, 全文.
审查员 毕雅超

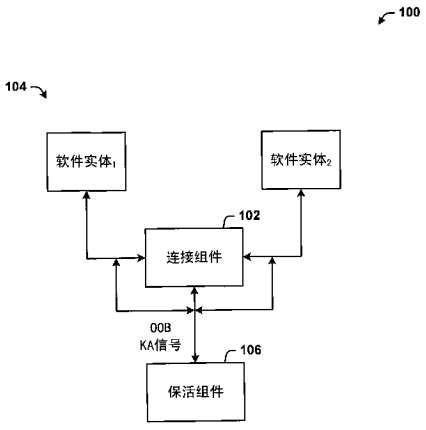
权利要求书 2 页 说明书 10 页 附图 10 页

(54)发明名称

用于与网络地址转换系统相关联的客户机的带外保活机制

(57)摘要

用于通过采用应用程序连接外部的带外(OOB)技术来维持网络地址转换(NAT)设备的连接状态,而不对底层本机应用程序施加附加要求的体系结构。该OOB解决方案可以应用于任意连接而不要求修改应用协议,并且对TCP和UDP有效。采用保活(KA)应用程序来作为注入KA分组的OOB机制,该KA分组对NAT设备而言表现为是来自本机连接的。这些注入分组欺骗NAT设备复位该连接的不活动定时器,但不欺骗本机应用程序或使其混淆,这对哄骗而言是易于忘记的。因此,连接将不会由于NAT超时而终止,并且因此客户机/服务器协议例如将不必生成伪造的活动分组来保持该连接活动。



CN 101622834 B

1. 一种方便连接管理的计算机实现的系统(100),包括 :

用于提供软件实体之间的任意通信连接的连接组件(102),所述连接组件包括网络地址转换 NAT 设备 ;以及

用于向所述连接组件发送带外 OOB 信号以维持所述连接的保活组件(106),所述保活组件监控所述连接组件的超时时间段,基于所述超时时间段采用保活刷新时间段,并基于所述刷新时间段来生成所述 OOB 信号并将其插入到所述连接中,以复位所述连接的超时定时器来维持所述连接,所述 OOB 信号是由所述保活组件插入到所述软件实体之间的连接中的保活分组。

2. 如权利要求 1 所述的系统,其特征在于,所述任意通信连接容纳传输层面向连接的端对端协议。

3. 如权利要求 1 所述的系统,其特征在于,所述任意通信连接容纳传输层无连接协议。

4. 如权利要求 1 所述的系统,其特征在于,所述 NAT 设备方便专用网与公共网的连接。

5. 如权利要求 1 所述的系统,其特征在于,所述保活组件是与所述软件实体不同的应用模块,所述保活组件的应用模块生成所述 OOB 信号并方便基于 TCP/IP 系统表的表活动来将所述 OOB 信号插入到所述软件实体之间的连接中。

6. 如权利要求 1 所述的系统,其特征在于,所述软件实体对应地驻留在客户机和服务器上,所述连接建立在所述软件实体之间。

7. 如权利要求 6 所述的系统,其特征在于,所述保活组件包括基于服务器的保活应用模块和基于客户机的保活应用模块,所述基于服务器的和基于客户机的保活应用模块通过所述连接组件来传递保活分组以维持所述连接。

8. 如权利要求 1 所述的系统,其特征在于,在所述 OOB 信号由所述连接组件处理之后,所述保活组件移除所述 OOB 信号。

9. 一种管理连接的计算机实现的方法,包括 :

在不同的系统的本机应用程序之间建立 NAT 连接(504),所述本机应用程序处理带内分组通信 ;以及

启动本机应用程序对应的一个或多个保活应用程序,所述保活应用程序执行带外分组活动,其中所述保活应用程序基于 NAT 超时时间段计算该 NAT 连接的刷新时间段,并基于 TCP/IP 系统表监控所述 NAT 连接的活动,基于所述刷新时间段自动地将带外 OOB 保活分组插入该 NAT 连接,以复位 NAT 超时定时器来维持该 NAT 连接。

10. 如权利要求 9 所述的方法,其特征在于,其中该 NAT 连接基于预定的连接策略用保活分组来操作。

11. 如权利要求 9 所述的方法,其特征在于, NAT 连接是经由传输控制协议(TCP)通信传输技术来促进的。

12. 如权利要求 9 所述的方法,其特征在于,还包括响应于感测 TCP/IP 系统表中的新项来启动所述本机应用程序的对应的保活应用程序。

13. 如权利要求 12 所述的方法,其特征在于,所述保活应用程序监控与所述本机应用程序相关联的对应的系统表中的连接状态,并基于所述连接状态停止发送所述保活分组。

14. 如权利要求 9 所述的方法,其特征在于,还包括 :

发现与所述本机应用程序中的至少一个相关联的元组,所述元组包括协议号、源 IP 地

址、源端口号、目的地 IP 地址、或目的地端口号中的至少两个；以及

基于利用所述元组的保活分组来复位 NAT 定时器。

15. 如权利要求 9 所述的方法，其特征在于，还包括通过 NAT 设备的已被处理的所述保活分组在到达所述本机应用程序之前被移除。

16. 如权利要求 9 所述的方法，其特征在于，还包括基于所述本机应用程序中的至少一个的带内活动来自动地启动保活应用程序。

17. 如权利要求 9 所述的方法，其特征在于，还包括经由一个或多个保活应用程序基于所采用的传输协议的类型来插入所述保活分组。

18. 一种计算机实现的系统（300），包括：

用于自动地在本机应用程序之间建立 NAT 连接的计算机实现的装置（306），所述本机应用程序处理带内分组通信；

用于自动地启动所述本机应用程序的对应的保活应用程序的计算机实现的装置（106），所述保活应用程序执行带外分组活动，所述保活应用程序基于 NAT 超时时间段来选择刷新时间段；

用于基于 TCP/IP 系统表来监控所述连接的活动的计算机实现的装置（106）；以及

用于响应于感测到不活动并基于刷新时间段来自动地将保活分组插入到所述连接中以复位 NAT 超时定时器的计算机实现的装置（106），所述保活分组基于 TCP 分组从两个保活应用程序插入，或基于 UDP 分组从所述保活应用程序中的一个插入。

用于与网络地址转换系统相关联的客户机的带外保活机制

[0001] 背景

[0002] 计算设备和连网的技术进步方便了对各种各样的信息和服务的访问，从而实际上允许从世界的任何地方进行访问。此外，随着计算机和便携式设备的数量的持续增加，连接性可以要求每一设备当其在网络上时都被唯一地标识。与支持为每一网络设备获取独立（或静态）IP 地址的附加花费相反，一种被称为网络地址转换 (NAT) 的技术允许路由器后的或内部（或专用）网络上的多个 IP 节点共享单个公共 IP 地址。换言之，提供了一种允许将一组未注册的 IP 地址用于内部网络通信并将另一组 IP 地址用于外部或公共通信的标准。

[0003] 通常，NAT 设备采用具有可配置超时时间段的连接超时定时器，以在本机应用程序之间映射连接状态。如果一特定 NAT 端口映射表项未被入站或出站通信使用超过了超时时间段，则该连接的 NAT 定时器期满并且该项从表中清除。一旦该项被清除，则 NAT 后的共享节点不能再通过该连接达到，并且必须发起新连接（例如由该共享节点）。

[0004] 防止 NAT 定时器超时（或期满）的一种常见机制被称为“保活”(KA) 或“心跳”处理。在保活下，以比 NAT 超时时间段短的时间间隔在该连接上生成无用通信以复位（或刷新）定时器，并且从而保持该连接活动。在使用电池电源作为主电源的便携式设备（例如智能电话）的情况下，常规保活技术影响电池寿命并生成大量的无线活动来保持连接活动。

[0005] 一种用于提供通过 NAT 的持久连接的解决方案是将保活机制作为本机应用协议的一部分来构建（带内解决方案）。然而，常规机制的缺点包括以下：必须修改底层本机应用协议来容纳 KA 机制；KA 机制不能被翻新到常规应用程序，并且需要部署应用程序升级；以及，对 KA 机制的每一次更新都影响核心应用协议并且因此必须被测试。

[0006] 另外，因为带内约束，优化常规 KA 机制是很困难的，带内约束包括：迫使 KA 分组大小不必要地大以容纳分层的本机应用头部（例如，大 HTTP（超文本标记语言）和 SOAP（简单对象访问协议）头部）；应用逻辑约束 KA 逻辑并可能要求附加网络连接；应用级可能不支持对故障模式和恢复的快速检测；应用程序开发者可能不具有必需的资源、时间、或专业知识来致力于完善基本上是系统级解决方案的方案；以及，适应并响应于移动漫游和不同的连网环境中的困难。

[0007] 概述

[0008] 以下提出了简化概述以便提供对在此描述的各新颖实施例的基本理解。本概述不是详尽的概览，并且它不旨在标识关键 / 重要的元素，也不旨在描绘其范围。其唯一的目的是以简化的形式来介绍一些概念，作为稍后提出的更为详细的描述的序言。

[0009] 所公开的体系结构提供一种用于通过采用带外 (OOB) 技术来保持网络地址转换 (NAT) 设备的连接状态活动的解决方案，该带外技术可在本机应用程序连接外部应用而不对该底层本机应用程序和 / 或应用协议施加任何要求或修改。本技术提供单独的保活 (KA) 应用程序，该保活应用程序通过将 KA 分组注入到本机应用程序来维持连接并且此后在该 KA 分组到达本机应用程序之前移除（例如丢弃）该 KA 分组，来以 OOB 方式与本机应用程序一起操作。在替换实现中，KA 分组不被移除而是由本机应用程序来处理（例如，过滤、丢

弃……)。

[0010] 该体系结构充分利用了常见NAT状态管理机制中的“逻辑空洞”。这些逻辑空洞不是“隐错”并且由此不被认为是安全漏洞,而仅仅是对内连连网设备所施加的约束的人工产物。一个逻辑空洞的性质与基于连接活动来维持NAT状态相关。NAT设备启动每一活动连接的超时定时器,并在每次该连接经历通信(例如分组活动)时复位该连接的超时(或不活动)定时器。如果在给定连接上未检测到通信,则超时定时器对该连接期满并且该连接失败。此外,NAT通常不验证通信的合法性(例如该通信所来自的端点)。

[0011] 利用该逻辑空洞,并且在一个示例性客户机/服务器环境中,可以采用在客户机和/或服务器上运行的第二网络KA应用程序作为OOB机制,来注入表现为来自本机连接的哄骗分组。这些注入的分组欺骗NAT设备复位该连接的不活动定时器,但不欺骗本机应用程序或使其混淆,这对哄骗而言是易于忘记的。因此,连接将不会由于NAT超时而终止,并且因此客户机/服务器协议将不必生成伪造的活动分组来保持该连接活动。

[0012] 该体系结构向通过NAT设备的任意不活动网络连接提供持续性,并且对诸如TCP(传输控制协议)等面向连接的端对端传输协议和诸如UDP(用户数据报协议)等无连接传输协议有效。

[0013] 为了实现前述及相关目的,此处结合以下说明书及附图来描述所公开的新颖体系结构的某些说明性方面。然而,这些方面仅指示了可利用此处公开的原理的各种方法中的少数几种,且旨在包括所有这些方面及其等效方面。结合附图阅读下面的详细描述,则其它优点和新颖特征将变得显而易见。

[0014] 附图简述

[0015] 图1示出根据一实施例的方便连接管理的计算机实现的系统。

[0016] 图2示出对连接的每一本机应用程序采用一保活(KA)应用程序的系统。

[0017] 图3示出用于使用带外(OOB)KA分组来维持连接的客户机/服务器系统。

[0018] 图4示出其中KA应用程序操作来处理多个连接的连接状态的替换系统。

[0019] 图5示出OOB KA管理的方法。

[0020] 图6示出基于连接策略的连接管理方法。

[0021] 图7示出基于传输协议来管理NAT连接不活动的方法。

[0022] 图8示出生成并利用KA分组来进行连接管理的方法。

[0023] 图9示出可用于执行所公开的KA体系结构的计算系统的框图。

[0024] 图10示出可采用OOB KA处理的示例性计算环境的示意性框图。

[0025] 详细描述

[0026] 所公开的体系结构提供一种用于通过采用带外(OOB)技术来保持网络地址转换(NAT)设备和/或软件的连接活动的解决方案,该带外技术可在本机应用程序连接外部应用而不对该本机应用程序施加任何要求或修改。该体系结构通过从在NAT设备的观点来看表现为本机连接的一部分的OOB源(例如应用程序)注入哄骗(或保活(KA))分组,来充分利用常见NAT状态管理机制中的“逻辑空洞”。这些注入的分组使NAT设备复位该连接的不活动定时器但不欺骗本机应用程序或使其混淆,这对哄骗而言是易于忘记的。因此,连接(例如,基于TCP(传输控制协议)或UDP(用户数据报协议))将不再由于NAT超时而终止,并且因此客户机/服务器协议例如将不再需要生成伪造的带内KA分组来保持该连接活动。

[0027] 现在参考附图，附图中相同的附图标记用于指代在全文中相同的元素。在以下描述中，为解释起见，描绘了众多具体细节以提供对本发明的全面理解。然而，显然，这些新颖实施例可以在没有这些具体细节的情况下实现。在其它情况下，以框图形式示出了公知的结构和设备以便于描述它们。

[0028] 一开始参考附图，图 1 示出根据一实施例的方便连接管理的计算机实现的系统 100。系统 100 包括用于在软件实体 104（示为软件实体 $_1$ 和软件实体 $_2$）之间提供任意通信连接的连接组件 102（例如 NAT 设备）。系统 100 还包括接口到连接组件 102 的、用于发送由连接组件 102 来处理以维持连接的 OOB KA 分组（或信号）的保活组件 106。

[0029] 在一个实现中，KA 组件 106 监控软件实体 104 所在的计算系统上的 TCP/IP 栈系统表活动。例如，新表项指示可向其中插入 KA 分组的新连接。可以监控软件实体所在的系统中的 TCP/IP 表。例如，可以监控客户机系统表。类似地，在涉及服务器的情况下，可以监控服务器系统 TCP/IP 表中的项活动（例如，移除或新项）。

[0030] 在替换和可任选实施例中，KA 组件 106 可以监控软件实体 104 中的一个或两者的连接分组活动，并基于此将活动 KA 分组插入到连接中。KA 分组可以由 KA 组件 106 外部地或在连接组件 102 的任一侧或两侧（例如，经由通过该连接路由分组的其它网络设备）插入到连接组件 102 的对应连接中，以使所插入的 KA 分组被连接组件 102 作为正常的带内通信来察觉。在连接组件 102 每次检测到分组（带内和 / 或保活）出现后，KA 分组随后复位该连接的连接定时器。

[0031] 系统表可由 KA 组件 106 来直接监控和 / 或经由连接组件 102 来间接监控。例如，如果表活动指示连接应被维持，则 KA 组件 106 将 KA 分组注入到该连接中，以使 KA 分组由连接组件 102 来处理以便复位连接定时器来维持该连接。

[0032] 在替换和可任选示例中，软件实体 104 中的一个或多个所监控的连接分组活动（或连接分组活动的缺乏）可被传递给 KA 组件 106，以使 KA 组件 106 向连接组件 102 发送 KA 分组，连接组件 102 随后将该 KA 分组插入到该连接中以用于自处理和超时定时器复位。在另一示例中，基于如由 KA 组件 106 所直接监控的连接分组不活动和保持该连接活动的期望，KA 组件 106 可以用信号通知软件实体 104 中的任一个或两者在该连接上生成带内 KA 分组，以复位该连接的超时定时器。在软件实体 104 是 KA 应用程序的情况下，KA 组件 106 可以用信号通知软件实体 104 中的任一个或两者将 OOB 分组插入到该连接中来维持该连接。应当理解，可以周期性地发送 KA 分组而不管表中的不活动或带内通信。

[0033] 系统 100 的一个实现包括作为连接组件 102 的一部分的 NAT 设备，以使软件实体 104 通过该 NAT 设备来彼此通信。软件实体 104（作为本机应用程序）经由该连接通过 NAT 来通信，从而通过规则的带内分组（只在本机应用程序之间）的通信创建活动连接。具有超时定时器的 NAT 设备基于从本机应用程序 104 接收到带内分组来不断地复位定时器。

[0034] 然而，偶尔，如果 NAT 设备在超时时段内未接收到带内分组，则 NAT 丢弃该连接并且应用程序需要通过该 NAT 设备重新建立连接。该体系结构通过提供至少一个 KA 应用程序（例如作为 KA 组件 106 的一部分）来解决该问题，该 KA 应用程序与本机应用程序 104 中的一个或多个一起启动以使该 KA 应用程序生成 KA 分组并将其插入到该连接中，从而使得 NAT 设备自动地复位超时定时器并且因此维持该连接。在从系统表中移除表项时，不再向该连接插入 KA 分组。

[0035] 在一个实现中，KA 组件 106 响应于感测到操作系统 TCP/IP 表中的新项来启动 KA 应用程序。因此，可以管理通过 NAT 来操作的多个不同的连接。在另一实现中，为每一本机应用程序（或软件实体 104）启动一个 KA 应用程序。在此，本机应用程序处理带内分组通信，而 KA 应用程序通过将 KA 分组插入到适当的 NAT 连接中来执行 OOB 分组活动以维持该连接，直到确定该连接应被断开为止。这将在图 2 中更详细地描述。

[0036] 图 2 示出对连接的每一本机应用程序采用一 KA 应用程序的系统 200。在此，KA 组件 106 包括两个 KA 应用程序 202：第一 KA 应用程序 204（示为 KA 应用程序 $_1$）和第二 KA 应用程序 206（示为 KA 应用程序 $_2$）。第一 KA 应用程序 204 和 / 或第二 KA 应用程序 206 中的一个或两者监控系统表项活动。在检测到新表项（例如在 TCP/IP 系统表中）时，KA 应用程序（204 和 / 或 206）中的一个或两者开始将 KA 分组插入到该连接中。

[0037] 在替换和可任选实施例中，在连接维持是基于分组通信而非表活动的情况下，第一 KA 应用程序 204 监控连接组件 102（例如 NAT 设备）和第一本机应用程序 208（示为本机应用程序 $_1$）之间的本机分组通信，和 / 或第二 KA 应用程序 206 监控连接组件 102 和第二本机应用程序 210（示为本机应用程序 $_2$）之间的本机分组通信。如此处所描述的，本机应用程序（208 和 210）被称为带内通信，而 KA 应用程序（204 和 206）被称为 OOB 通信。通过监控与第一本机应用程序系统相关联的系统表，可以发现第一本机应用程序的网络 5 元组（例如，协议号、源 IP 地址、源端口、目的地 IP 地址和目的地端口）。基于该信息，第一 KA 应用程序 204 可以观察并基于所观察的连接组件 102 的超时来采用所需的 KA 刷新时间段。KA 刷新时间段比连接组件 102 的超时时间段短，以便 KA 分组在该连接的超时时间段期满之前发送。例如，如果超时时间段是 15 分钟，则可以将刷新选为 10 分钟（或小于超时时间段的任何其它合适值）。

[0038] 在一个替换和可任选操作中，基于刷新时间段，第一 KA 应用程序 204 会在连接组件 102 的每次超时时间段期满之前将 KA 分组注入到连接中。当然，这是基于第一本机应用程序 208 的分组活动的。换言之，如果第一本机应用程序 208 例如通过从第一本机应用程序 208 到第一 KA 应用程序 204 的信号来指示不再需要与第二本机应用程序 210 通信，则第一 KA 应用程序 204 将停止向该连接注入 KA 分组。因此，连接组件 102 随后将使该连接超时并且该连接将失败。

[0039] 在一个实施例中，在第一 KA 应用程序 204 正在发送 KA 分组时，第二 KA 应用程序 206 将移除该 KA 分组。因此，第二本机应用程序 210 将不再需要不必要地处理 KA 分组。

[0040] 根据类似的和可任选的操作，通过监控第二本机应用程序 210 和连接组件 102 之间的分组通信而非系统表，第二 KA 应用程序 206 发现第二本机应用程序的网络 5 元组（例如，协议号、源 IP 地址、源端口、目的地 IP 地址和目的地端口）。基于该信息，第二 KA 应用程序 206 可以观察并基于所观察的连接组件 102 的超时来采用合适的 KA 刷新时间段。基于该刷新时间段，第二 KA 应用程序 206 将在每次超时时间段期满之前向该连接注入 KA 分组。当然，这是基于第二本机应用程序 210 的活动的。换言之，如果第二本机应用程序 210 指示不再需要与第一本机应用程序 208 的通信，则第二 KA 应用程序 206 将停止向该连接注入 KA 分组。因此，连接组件 102 随后将使该连接超时并且该连接将失败。

[0041] 在另一实施例中，在第二 KA 应用程序 206 正在发送 KA 分组时，第一 KA 应用程序 204 将移除该 KA 分组。因此，第一本机应用程序 208 将不必处理 KA 分组。

[0042] 根据另一操作，通过监控第一和第二本机应用程序 (208 和 210) 两者与连接组件 102 之间的分组通信，对应的第一和第二 KA 应用程序 (204 和 206) 发现本机应用程序的网络 5 元组。基于该信息，第一和第二 KA 应用程序 (204 和 206) 可以观察并基于所观察的连接组件 102 的超时来采用所需的 KA 刷新时间段。基于该刷新时间段，第一和 / 或第二 KA 应用程序 (204 和 206) 将在每次超时时间段期满之前向该连接注入 KA 分组。当然，这是基于对应的第一和第二本机应用程序 (208 和 210) 的活动的。在又一实现中，只要在 NAT 超时期满的某点处，连接组件 102 的两侧都被刷新，则两个 KA 应用程序 (204 和 206) 可以独立地操作。

[0043] 换言之，根据该可任选实现，如果第二本机应用程序 210 例如通过从第二本机应用程序 210 到第二 KA 应用程序 206 的信号来指示不再需要与第一本机应用程序 208 的通信，则第二 KA 应用程序 206 将停止向连接注入 KA 分组。类似地，如果第一本机应用程序 208 指示不再需要与第二本机应用程序 210 的通信，则第一 KA 应用程序 204 将停止向该连接注入 KA 分组。因此，连接组件 102 随后将使该连接超时并且该连接将失败。当第一和第二 KA 应用程序 (分别是 204 和 206) 两者都在发送 KA 分组时，相对的第二和第一 KA 应用程序 (分别是 206 和 204) 可以移除所接收到的 KA 分组。因此，第一第二本机应用程序 (208 和 210) 将不必被配置来处理 KA 分组。

[0044] 图 3 示出用于使用 OOB KA 分组来维持连接的客户机 / 服务器系统 300。更具体地，在客户机 / 服务器场景中，客户机 304 的客户机本机应用程序 302 打开通过 NAT 设备 306 到服务器 310 的服务器本机应用程序 308 的持久 UDP 或 TCP 连接。该体系结构对诸如 TCP 等面向连接的端对端传输协议和诸如 UDP 等无连接传输协议有效。客户机 304 还可以包括通过其发生通信的防火墙、过滤或多路复用组件 312(此后统称为防火墙 312)。通信经由客户机 TCP/IP 栈和表 314，通过 NAT 设备 306、服务器 TCP/IP 栈和表 316、以及服务器防火墙 318、到服务器本机应用程序 308 的连接来进行。栈 (314 和 316) 具有相关联的 TCP/IP 协议系统表，该表用所建立的每一新连接的新表项来更新并丢弃被丢弃的连接的表项。

[0045] 根据一个实现，在客户机 304 和服务器 310 这两侧都启动 KA 应用程序 (共同描述为 KA 组件 106)。客户机 KA 应用程序 320 在客户机 304 上启动，且服务器 KA 应用程序 322 在服务器 310 上启动。可以理解，KA 组件应用程序 (320 和 322) 可以用操作系统来启动以作为后台进程持续运行。如上所述，KA 组件 106(客户机和服务器 KA 应用程序中的一个或两者 (320 和 / 或 322)) 可以经由与 TCP/IP 栈 (314 和 316) 相关联的 TCP/IP 表来发现连网 5 元组 (例如，协议号、源 IP 地址、源端口、目的地 IP 地址、以及目的地端口)。

[0046] KA 应用程序 (320 和 322) 可以共同或独立地观察并 (基于所观察的 NAT 超时) 采用所需的 KA 刷新时间段。例如，假定 NAT 设备 306 后 (例如在专用侧) 的客户机 304 打开到 (在公共侧) 服务器 310 的 TCP 连接，并且此后维持安静 (无分组活动)。建立该连接在客户机 TCP/IP 系统表中产生新表项。在没有 KA 应用程序 106 的情况下，如在常规实现中，NAT 设备 306 将使该连接状态超时并致使该 TCP 连接无用。利用以所描述的 OOB 方式操作的 KA 组件 106 确保了该 TCP 连接将不会由于 NAT 超时而终止，并且因此客户机 / 服务器协议将不必生成“伪造”带内活动来保持该连接活动。如果所观察的 NAT 超时例如是 15 分钟，则刷新时间段 (或值) 可以小于 15 分钟 (例如 10 分钟)。一般而言，采用小于所观察的 NAT 设备超时时间段的 KA 刷新时间段。

[0047] 在操作中，KA 应用程序 (320 和 322) 共同地或独立地（取决于传输协议）从客户机 304、服务器 310 或客户机 304 和服务器 310 两者发送 KA（或哄骗）连接分组。KA 组件 106 运作来在 NAT 设备 306 的接收侧移除哄骗分组，从而通过处理 KA 分组来消除接收本机应用程序中的混淆。

[0048] 在替换实现中，在本机应用程序（客户机本机应用程序 302 或服务器本机应用程序 308) 足够稳健来处理哄骗分组而不会混淆（或造成出错）时，不执行 KA 组件 106 对哄骗分组的移除。这可以包括识别和丢弃哄骗分组。例如，可以在接收侧通过检查分组数据中唯一地定义哄骗分组的信息来过滤和 / 或移除 KA 分组。KA 分组可以是零净荷分组（只有头部）。还可以使用其它方式。在每次接收到哄骗分组后（以及接收到本机分组后），NAT 设备 306 复位 NAT 连接超时。由于 TCP/IP 协议的性质，所以哄骗是在原始 IP 层执行的，因为 UDP/TCP 协议不允许发送者和接收者两者的多个应用程序都绑定到相同的 5 元组。

[0049] KA 组件 106 可以通过与相应的防火墙 (312 和 318) 和 / 或系统 TCP/IP 栈和表 (34 和 316) 通信来发现本机应用程序 5 元组另外，KA 分组移除可以由相应的接收防火墙 (312 和 318) 使用过滤功能来实现。此外，系统 300 不限于客户机 / 服务器场景，而还适用于对等拓扑结构。

[0050] 图 4 示出其中 KA 应用程序操作来处理多个连接的连接状态的替换系统 400。系统 400 包括寻求通过 NAT 设备 306 与第二系统 404 通信的第一系统 402（例如，便携式计算机）。第一系统 402 包括两个本机应用程序：第一本机应用程序 406 和第二本机应用程序 408。第一系统 402 还包括接口到第一和第二本机应用程序 (406 和 408) 的第一 KA 应用程序 410，其经由第一系统 402 的 TCP/IP 系统表项来监控第一系统 402 的本机应用程序系统间 (402 和 404) 活动。可任选地，第一 KA 应用程序 410 还可以经由 NAT 设备 306 来监控连接的连接状态。

[0051] 类似地，第二系统 404（例如 web 服务器）通过 NAT 设备 306 与第一系统 402 通信。在该具体示例中，第二系统 404 包括两个本机应用程序：第三本机应用程序 412 和第四本机应用程序 414。第二系统 404 还包括接口到第三和第四本机应用程序 (412 和 414) 的第二 KA 应用程序 416，其经由第二系统 404 的 TCP/IP 系统表项来监控第二系统 404 的本机应用程序活动。可任选地，第二 KA 应用程序 416 还可以经由 NAT 设备 306 来监控 NAT 连接的连接状态。

[0052] 在该示例中，第一和第三本机应用程序 (406 和 412) 打开通过 NAT 设备 306 的第一连接（示为连接 $_1$），并且第二和第四本机应用程序 (408 和 414) 打开通过 NAT 设备 306 的第二连接（示为连接 $_2$）。基于第一系统 402 中的新 TCP/IP 系统表项和 / 或第二系统 404 中的新 TCP/IP 系统表项，第一和第二 KA 应用程序 (410 和 416) 向对应的第一和第二连接提供 KA 分组，以维持所需的第一和 / 或第二连接的连接状态。

[0053] 在其中任一系统 (402 或 404) 中都没有本机应用程序活动的初始状态中，不启动 KA 应用程序 (410 和 416)。在第一本机应用程序 406 打开通过 NAT 设备 306 的第一连接时，第一 KA 应用程序 410 启动并采用第一连接 KA 分组的刷新时间段。例如，第一连接到第三本机应用程序 412 是活动的；然而，如果该连接是不活动的并且期望该第一连接不应是不活动的，则第一 KA 应用程序 410 将自动地向该第一连接插入第一连接 KA 分组以维持该第一连接。在检测到第三本机应用程序 412 中的活动时，第二 KA 应用程序 416（现在是接收

KA 应用程序）将从分组流中过滤出所接收到的 KA 分组。因此，第三本机应用程序 412 可以接收分组流而不受 KA 分组处理和 / 或过滤的妨碍。

[0054] 如果第二本机应用程序 408 此时被激活，并且打开到第四本机应用程序 414 的第二连接，则因为第一 KA 应用程序 410 已经知道 NAT 设备 306 的刷新时间段，因此只要第二连接（连接 $_2$）需要不活动控制，则对于该第二连接将 KA 连接维持应用于 NAT 设备 306。因此，第一 KA 应用程序 410 可以管理通过单个 NAT 设备 306 的多个连接。在替换操作中，第一 KA 应用程序 410 管理第一连接，而第二系统 404 的第二 KA 应用程序 410 管理第二连接。可以看到，在具有用于多个连接的多个端口的 NAT 设备的典型实现中，可以执行多个连接 KA 管理。

[0055] 图 5 示出 OOB KA 管理方法。尽管出于解释简明的目的，此处例如以流图或流程图形式示出的一个或多个方法被示出并描述为一系列动作，但是可以理解和明白，这些方法不受动作的次序的限制，因为根据本发明，某些动作可以按与此处所示并描述的不同的次序和 / 或与其它动作同时发生。例如，本领域技术人员将会明白并理解，方法可被替换地表示为一系列相互关联的状态或事件，诸如以状态图的形式。此外，并非方法中的所有所示动作都是对于新颖实现所必需的。

[0056] 在 500 处，打开不同系统的本机应用程序之间的 NAT 连接。在 502 处，确定该 NAT 连接的刷新时间段。换言之，KA 应用程序可包括将基于其传送 KA 分组的刷新值表。刷新值可被硬编码（例如每 30 秒）在 KA 应用程序中，或 KA 应用程序可以使用预计算的值。可任选地，刷新时间段可由相关联的 KA 应用程序基于 NAT 超时时间段来自动地计算。在 504 处，基于系统表活动来监控连接。在 506 处，使用 KA 应用程序基于所选择的刷新值来自动地在发送侧将 KA 分组插入到连接。在 508 处，在接收侧按需移除 KA 分组。换言之，不要求接收 KA 应用程序在接收侧移除 KA 分组。

[0057] 图 6 示出基于连接策略的连接管理方法。在 600 处，打开本机应用程序之间的 NAT 连接。在 602 处，相关联的 KA 应用程序基于 NAT 超时时间段来选择刷新值。在 604 处，获取并处理与该连接相关联的策略。在 606 处，使用 KA 应用程序基于所选择的刷新值来自动地在发送侧将 KA 分组插入到连接。在 608 处，根据策略用 KA 分组操作该连接。换言之，该策略可以指示该连接保持打开预定一段时间并在该时间期满之后关闭该连接，而不管带内或 OOB 分组通信是否已经终止。

[0058] 图 7 示出基于类型传输协议来管理 NAT 连接不活动的方法。在 700 处，打开本机应用程序之间的 NAT 连接。在 702 处，基于本机应用程序的活动，启动对应的 KA 应用程序中的一个或多个。在 704 处，KA 应用程序中的一个或多个基于 NAT 超时时间段来选择刷新时间段。在 706 处，KA 应用程序基于栈表活动来监控对应的本机应用程序连接。在 708 处，基于 TCP 分组的先前通信，从 KA 应用程序中的每一个将 KA 分组自动地插入到该连接。另选地，在 710 处，基于 UDP 分组的先前通信，从 KA 应用程序中的一个或两者将 KA 分组自动地插入到该连接。因为 TCP 是面向连接的端对端传输协议，所以需要两个 KA 应用程序都操作来插入 KA 分组和移除 KA 分组。因为 UDP 是无连接传输协议，所以在大多数情况下，只需要 KA 应用程序中的一个操作来将 KA 分组插入到 NAT 连接中。

[0059] 图 8 示出生成并利用 KA 分组来进行连接管理的方法。在 800 处，一个本机应用程序打开通过 NAT 设备的到另一本机应用程序的连接。在 802 处，在启动 KA 应用程序之后，

KA 应用程序中的一个或多个利用刷新时间段。在 804 处，发起发现过程来发现本机应用程序的连网 5 元组的发现过程。这可以经由 TCP/IP 表来进行。在 806 处，使用 5 元组信息来为特定连接构造 KA 分组。在 808 处，基于刷新时间段将 KA 分组插入到该连接以复位 NAT 超时定时器。在 810 处，通过 NAT 设备的已被处理的 KA 分组在到达本机应用程序之前被移除。

[0060] 如在本申请中所使用的，术语“组件”和“系统”旨在表示计算机相关的实体，其可以是硬件、硬件和软件的组合、软件、或者执行中的软件。例如，组件可以是但不限于，在处理器上运行的进程、处理器、硬盘驱动器、多个（光和 / 或磁存储介质的）存储驱动器、对象、可执行代码、执行的线程、程序、和 / 或计算机。作为说明，运行在服务器上的应用程序和服务器都可以是组件。一个或多个组件可以驻留在进程和 / 或执行的线程内，且组件可以位于一台计算机内上 / 或分布在两台或更多的计算机之间。

[0061] 现在参考图 9，示出了可用于执行所公开的 KA 体系结构的计算系统 900 的框图。为了提供用于其各方面的附加上下文，图 9 及以下讨论旨在提供对其中可实现本体系结构的各方面的合适的计算系统 900 的简要概括描述。尽管以上描述是在可在一个或多个计算机上运行的计算机可执行指令的一般上下文中进行的，但是本领域的技术人员将认识到，本体系结构也可结合其它程序模块和 / 或作为硬件和软件的组合来实现。

[0062] 一般而言，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、组件、数据结构等等。此外，本领域的技术人员可以理解，本发明的方法可用其它计算机系统配置来实施，包括单处理器或多处理器计算机系统、小型机、大型计算机、以及个人计算机、手持式计算设备、基于微处理器的或可编程消费电子产品等，其每一个都可操作上耦合到一个或多个相关联的设备。

[0063] 所示各方面也可以在其中某些任务由通过通信网络链接的远程处理设备来执行的分布式计算环境中实践。在分布式计算环境中，程序模块可以位于本地和远程存储器存储设备中。

[0064] 计算机通常包括各种计算机可读介质。计算机可读介质可以是可由计算机访问的任何可用介质，且包括易失性和非易失性介质、可移动和不可移动介质。作为示例而非限制，计算机可读介质可以包括计算机存储介质和通信介质。计算机存储介质包括以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据之类的信息的任意方法或技术实现的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括但不限于 RAM、ROM、EEPROM、闪存或者其它存储器技术、CD-ROM、数字视频盘 (DVD) 或其它光盘存储、磁带盒、磁带、磁盘存储或其它磁存储设备、或可以用于存储所需信息并且可以由计算机访问的任何其它介质。

[0065] 再次参考图 9，用于实现各方面的示例性计算系统 900 包括计算机 902，计算机 902 包括处理单元 904、系统存储器 906 和系统总线 908。系统总线 908 向包括但不限于系统存储器 906 的各系统组件提供到处理单元 904 的接口。处理单元 904 可以是市场上可购买到的各种处理器中的任意一种。双微处理器和其它多处理器体系结构也可用作处理单元 904。

[0066] 系统总线 908 可以是若干种总线结构中的任一种，这些总线结构还可互连到存储器总线（带有或没有存储器控制器）、外围总线、以及使用各类市场上可购买到的总线体系结构中的任一种的局部总线。系统存储器 906 包括只读存储器 (ROM) 910 和随机存取存储

器 (RAM)912。基本输入 / 输出系统 (BIOS) 储存在诸如 ROM、EPROM、EEPROM 等非易失性存储器 910 中，其中 BIOS 包含帮助诸如在启动期间在计算机 902 内的元件之间传输信息的基本例程。RAM 912 还可包括诸如静态 RAM 等高速 RAM 来用于高速缓存数据。

[0067] 计算机 902 还包括内置硬盘驱动器 (HDD)914（例如，EIDE、SATA），该内置硬盘驱动器 914 还可被配置成在合适的机壳（未示出）中供外部使用；磁软盘驱动器 (FDD)916（例如，从可移动磁盘 918 中读取或向其写入）；以及光盘驱动器 920（例如，从 CD-ROM 盘 922 中读取，或从诸如 DVD 等其它高容量光学介质中读取或向其写入）。硬盘驱动器 914、磁盘驱动器 916 和光盘驱动器 920 可分别通过硬盘驱动器接口 924、磁盘驱动器接口 926 和光盘驱动器接口 928 连接到系统总线 908。用于外置驱动器实现的接口 924 包括通用串行总线 (USB) 和 IEEE 1394 接口技术中的至少一种或两者。

[0068] 驱动器及其相关联的计算机可读介质提供了对数据、数据结构、计算机可执行指令等的非易失性存储。对于计算机 902，驱动器和介质容纳适当的数字格式的任何数据的存储。尽管以上对计算机可读介质的描述涉及 HDD、可移动磁盘以及诸如 CD 或 DVD 等可移动光学介质，但是本领域的技术人员应当理解，示例性操作环境中也可使用可由计算机读取的任何其它类型的介质，诸如 zip 驱动器、磁带盒、闪存卡、盒式磁带等等，并且任何这样的介质可包含用于执行所公开的方法的计算机可执行指令。

[0069] 多个程序模块可存储在驱动器和 RAM 912 中，包括操作系统 930、一个或多个应用程序 932、其它程序模块 934 和程序数据 936。所有或部分操作系统、应用程序、模块和 / 或数据也可被高速缓存在 RAM 912 中。应该明白，本体系结构可以用各种市场上可购得的操作系统或操作系统的组合来实现。应用程序 932 和 / 或模块 934 可包括本机应用程序、KA 应用程序、和 / 或先前描述的 KA 组件。

[0070] 用户可以通过一个或多个有线 / 无线输入设备，例如键盘 938 和诸如鼠标 940 等定点设备将命令和信息输入到计算机 902 中。其它输入设备（未示出）可包括话筒、IR 遥控器、操纵杆、游戏手柄、指示笔、触摸屏等等。这些和其它输入设备通常通过耦合到系统总线 904 的输入设备接口 942 连接到处理单元 908，但也可通过其它接口连接，如并行端口、IEEE 1394 串行端口、游戏端口、USB 端口、IR 接口等等。

[0071] 监视器 944 或其它类型的显示设备也经由接口，诸如视频适配器 946 连接至系统总线 908。除了监视器 944 之外，计算机通常包括诸如扬声器和打印机等其它外围输出设备（未示出）。

[0072] 计算机 902 可使用经由有线和 / 或无线通信至一个或多个远程计算机，诸如远程计算机 948 的逻辑连接在网络化环境中操作。远程计算机 948 可以是工作站、服务器计算机、路由器、个人计算机、便携式计算机、基于微处理器的娱乐设备、对等设备或其它常见的网络节点，并且通常包括以上相对于计算机 902 描述的许多或所有元件，尽管为简明起见仅示出了存储器 / 存储设备 950。所描绘的逻辑连接包括到局域网 (LAN)952 和 / 或例如广域网 (WAN)954 等更大的网络的有线 / 无线连接。这一 LAN 和 WAN 连网环境常见于办公室和公司，并且方便了诸如内联网等企业范围计算机网络，所有这些都可连接到例如因特网等全球通信网络。

[0073] 当在 LAN 网络环境中使用时，计算机 902 通过有线和 / 或无线通信网络接口或适配器 956 连接到局域网 952。适配器 956 可以方便到 LAN 952 的有线或无线通信，并且还可

包括其上设置的用于与无线适配器 956 通信的无线接入点。

[0074] 当在 WAN 连网环境中使用时，计算机 902 可包括调制解调器 958，或连接到 WAN 954 上的通信服务器，或具有用于通过 WAN 954，诸如通过因特网建立通信的其它装置。或为内置或为外置以及有线或无线设备的调制解调器 958 经由串行端口接口 942 连接到系统总线 908。在网络化环境中，相对于计算机 902 所描述的程序模块或其部分可以存储在远程存储器 / 存储设备 950 中。应该理解，所示网络连接是示例性的，并且可以使用在计算机之间建立通信链路的其它手段。

[0075] 计算机 902 可用于与操作上设置在无线通信中的任何无线设备或实体通信，这些设备或实体例如有打印机、扫描仪、台式和 / 或便携式计算机、便携式数据助理、通信卫星、与无线可检测标签相关联的任何一个设备或位置（例如，公用电话亭、报亭、休息室）以及电话机。这至少包括 Wi-Fi 和蓝牙 ™ 无线技术。由此，通信可以如对于常规网络那样是预定义结构，或者仅仅是至少两个设备之间的自组织 (ad hoc) 通信。

[0076] 现在参考图 10，示出了可采用 OOB KA 处理的示例性计算环境 1000 的示意性框图。系统 1000 包括一个或多个客户机 1002。客户机 1002 可以是硬件和 / 或软件（例如，线程、进程、计算设备）。例如，客户机 1002 可容纳 cookie 和 / 或相关联的上下文信息。

[0077] 系统 1000 还包括一个或多个服务器 1004。服务器 1004 也可以是硬件和 / 或软件（例如，线程、进程、计算设备）。服务器 1004 可以例如通过使用本体系结构来容纳线程以执行变换。在客户机 1002 和服务器 1004 之间的一种可能的通信能够以适合在两个或多个计算机进程之间传输的数据分组的形式进行。数据分组可包括例如 cookie 和 / 或相关联的上下文信息。系统 1000 包括可以用来使客户机 1002 和服务器 1004 之间通信更容易的通信框架 1006（例如，诸如因特网等全球通信网络）。

[0078] 通信可经由有线（包括光纤）和 / 或无线技术来促进。客户机 1002 操作上被连接到可以用来存储对客户机 1002 本地的信息（例如，cookie 和 / 或相关联的上下文信息）的一个或多个客户机数据存储 1008。同样地，服务器 1004 可在操作上连接到可以用来存储对服务器 1004 本地的信息的一个或多个服务器数据存储 1010。

[0079] 客户机 1002 和服务器 1004 两者都可以包括监控诸如 NAT 路由器、网关等网络接口（未示出）的 KA 应用程序。如上所述，客户机 1002 能以对等方式互连，这样通过使用本地 KA 应用程序，连接状态管理可以在客户机中的一个或两者的内部。

[0080] 以上所描述的包括所公开的体系结构的各示例。当然，描述每一个可以想到的组件和 / 或方法的组合是不可能的，但本领域内的普通技术人员应该认识到，许多其它组合和排列都是可能的。因此，本新颖体系结构旨在涵盖所有这些落入所附权利要求书的精神和范围内的更改、修改和变化。此外，就在说明书或权利要求书中使用术语“包括”而言，这一术语旨在以与术语“包含”在被用作权利要求书中的过渡此时所解释的相似的方式为包含性的。

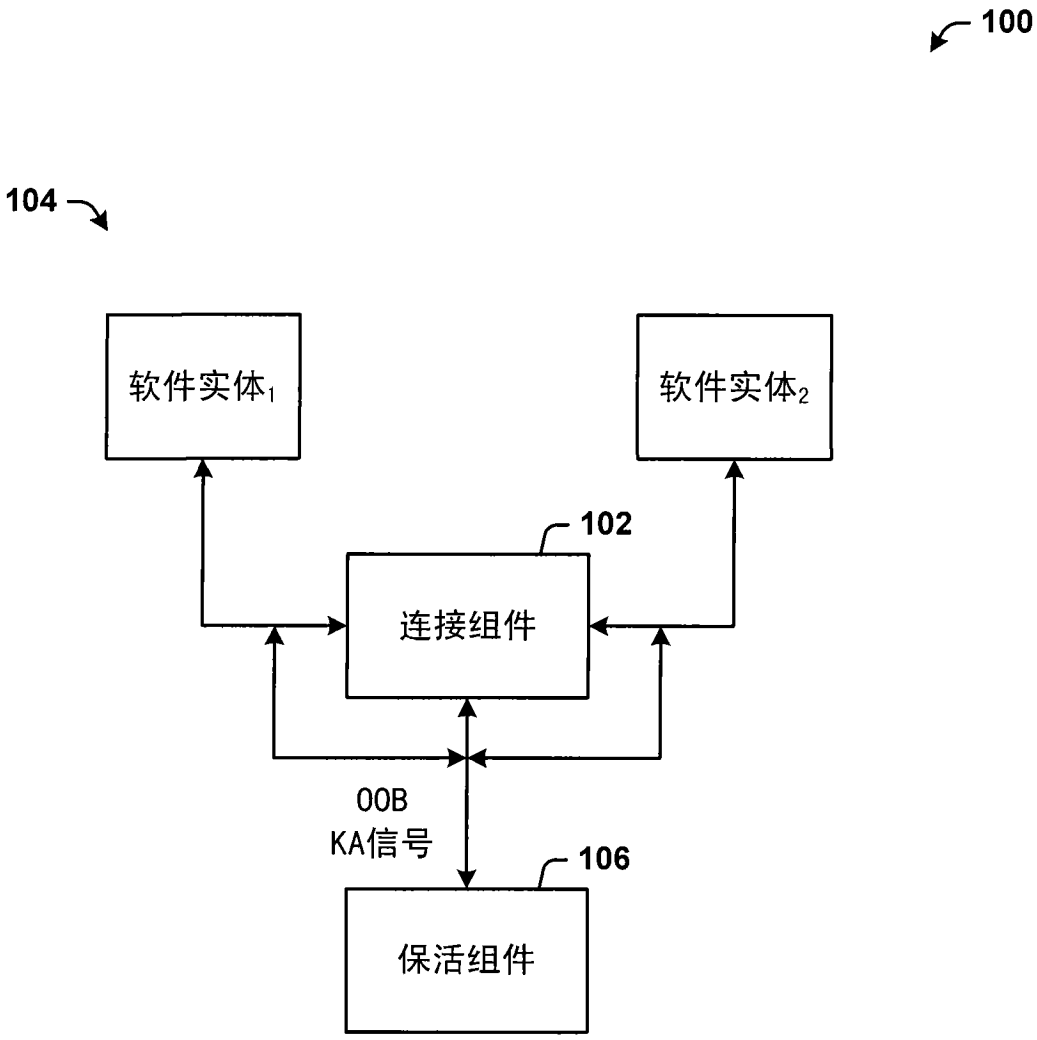


图 1

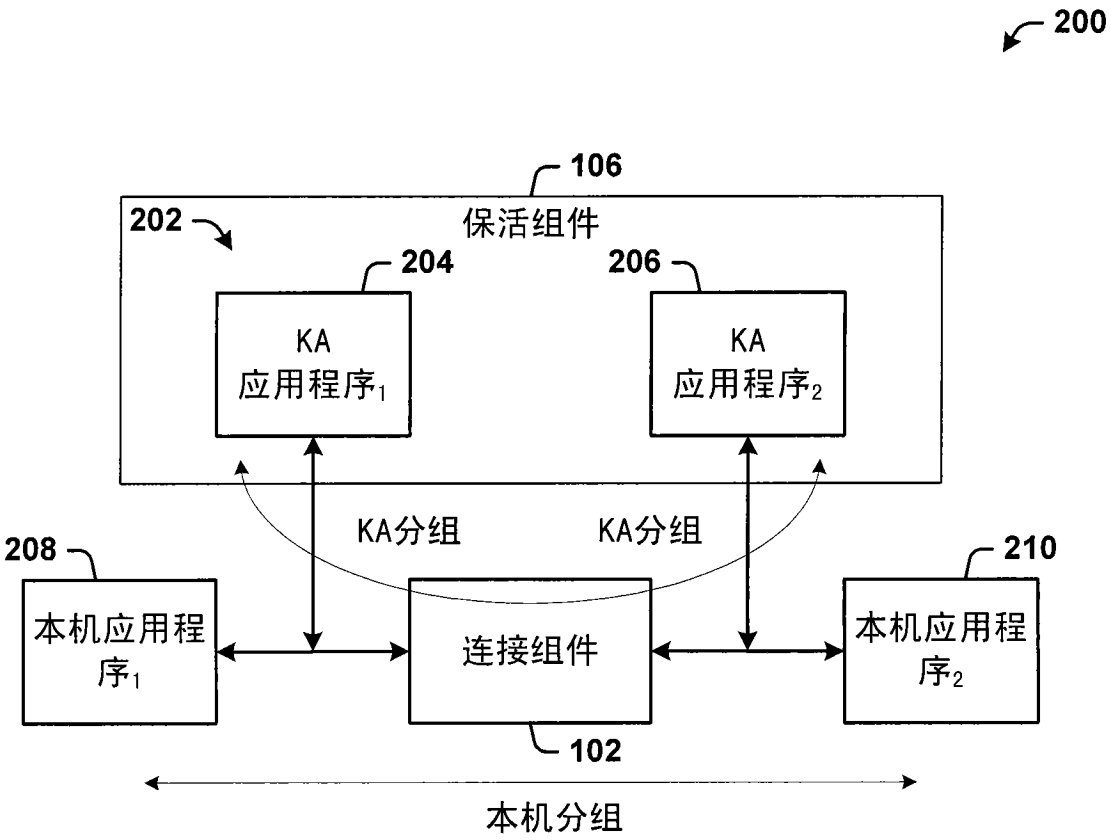

200
106
保活组件
202
204
206
KA
应用程序1
KA
应用程序2
KA分组
KA分组
208
210
本机应用程
序1
连接组件
本机应用程
序2
102
本机分组

图 2

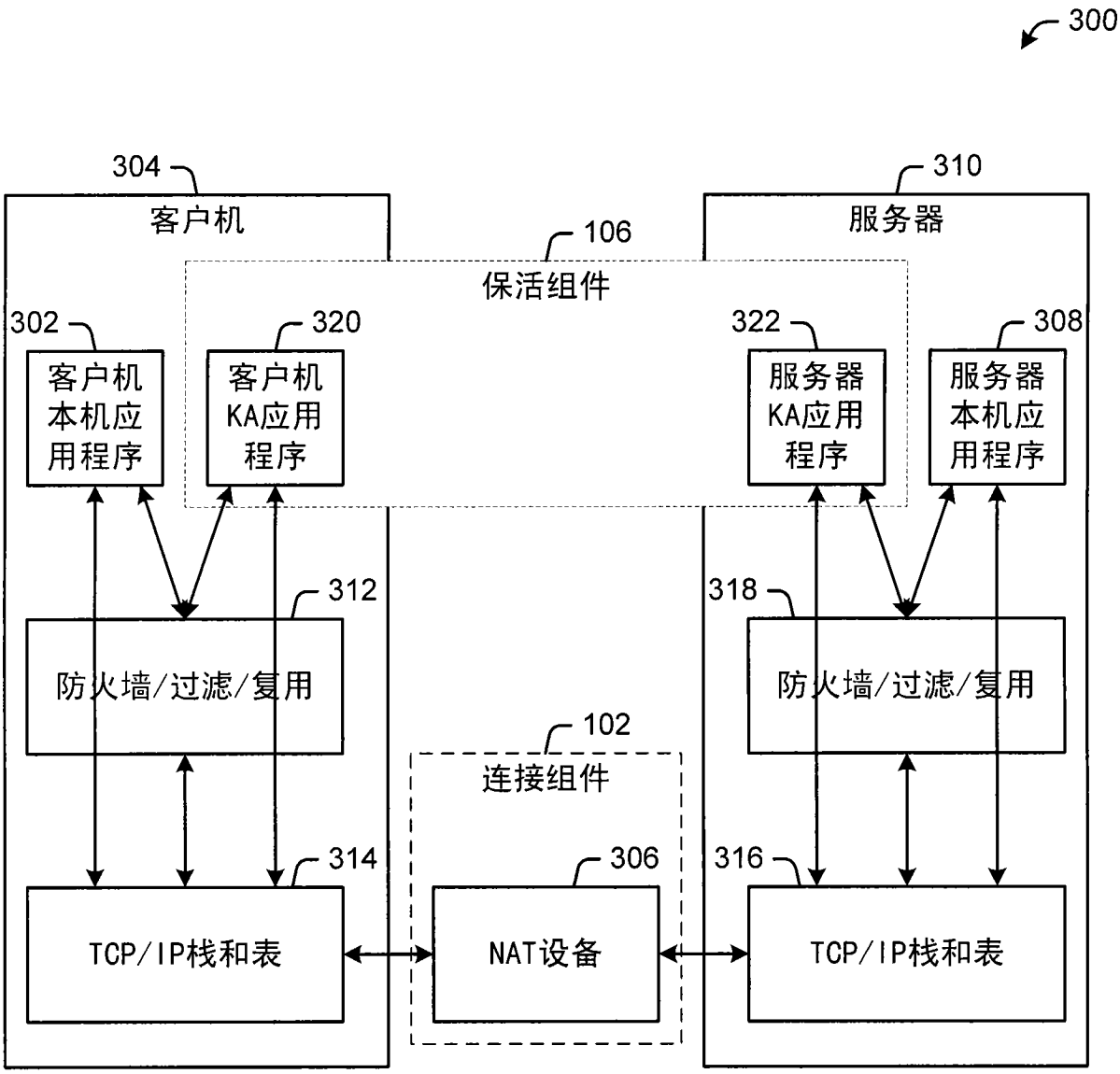

300
304
客户机
310
服务器
106
保活组件
302
客户机本机应用程序
320
客户机KA应用程序
322
服务器KA应用程序
308
服务器本机应用程序
312
防火墙/过滤/复用
318
防火墙/过滤/复用
102
连接组件
314
TCP/IP栈和表
306
NAT设备
316
TCP/IP栈和表

图 3

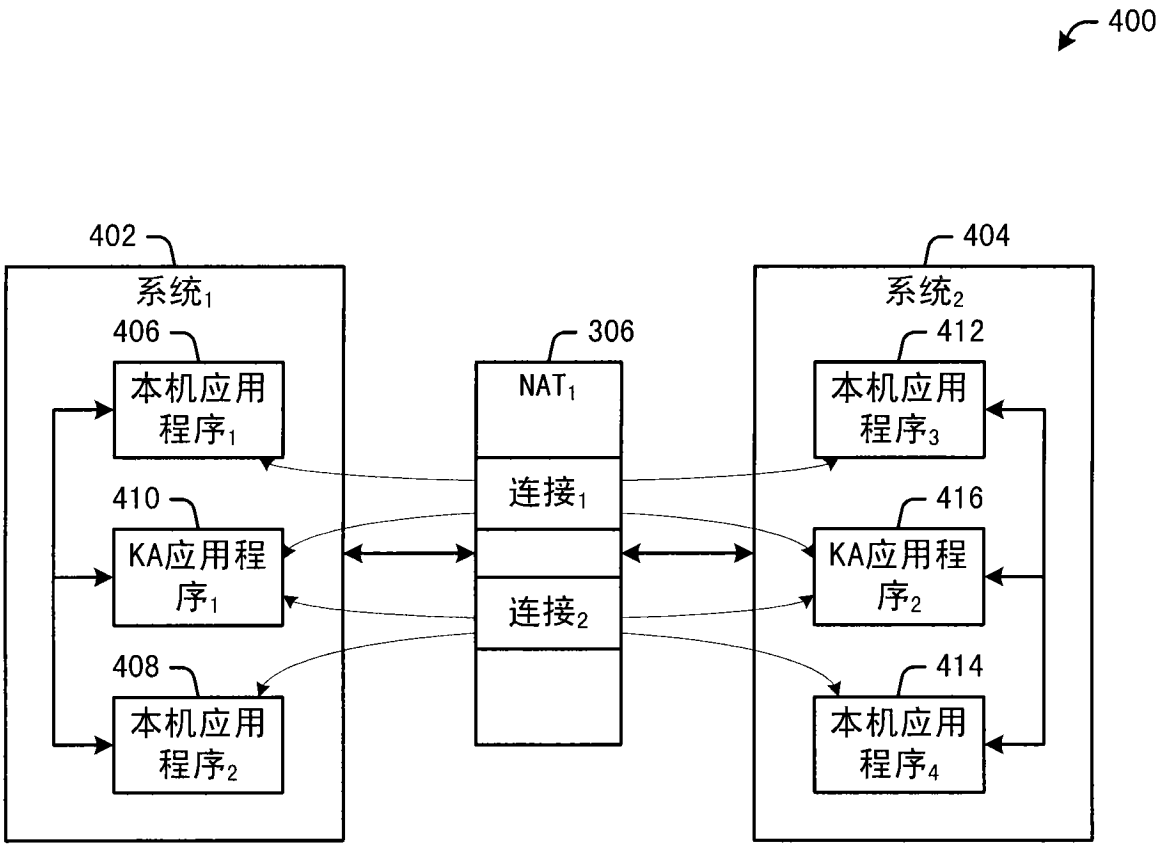

400
402
系统1
406
本机应用程序1
410
KA应用程序1
408
本机应用程序2
306
NAT1
连接1
连接2
404
系统2
412
本机应用程序3
416
KA应用程序2
414
本机应用程序4

图 4

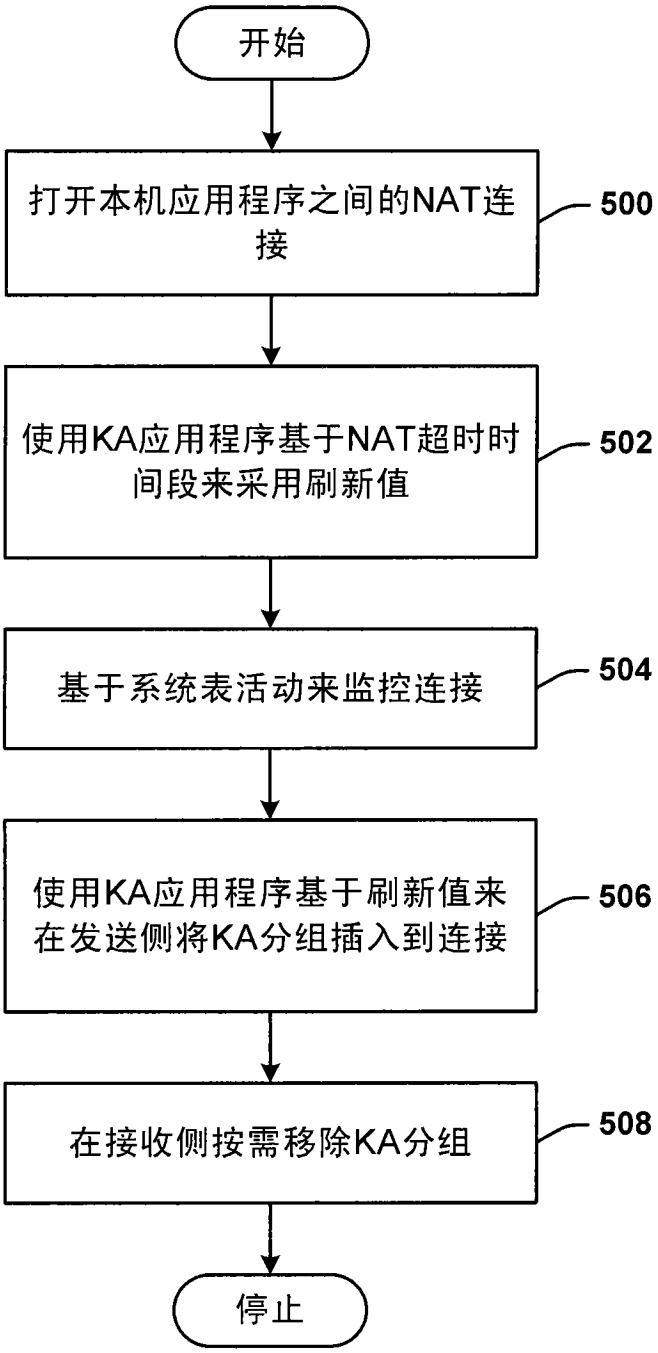

开始
打开本机应用程序之间的NAT连接
500
使用KA应用程序基于NAT超时时间段来采用刷新值
502
基于系统表活动来监控连接
504
使用KA应用程序基于刷新值来在发送侧将KA分组插入到连接
506
在接收侧按需移除KA分组
508
停止

图 5

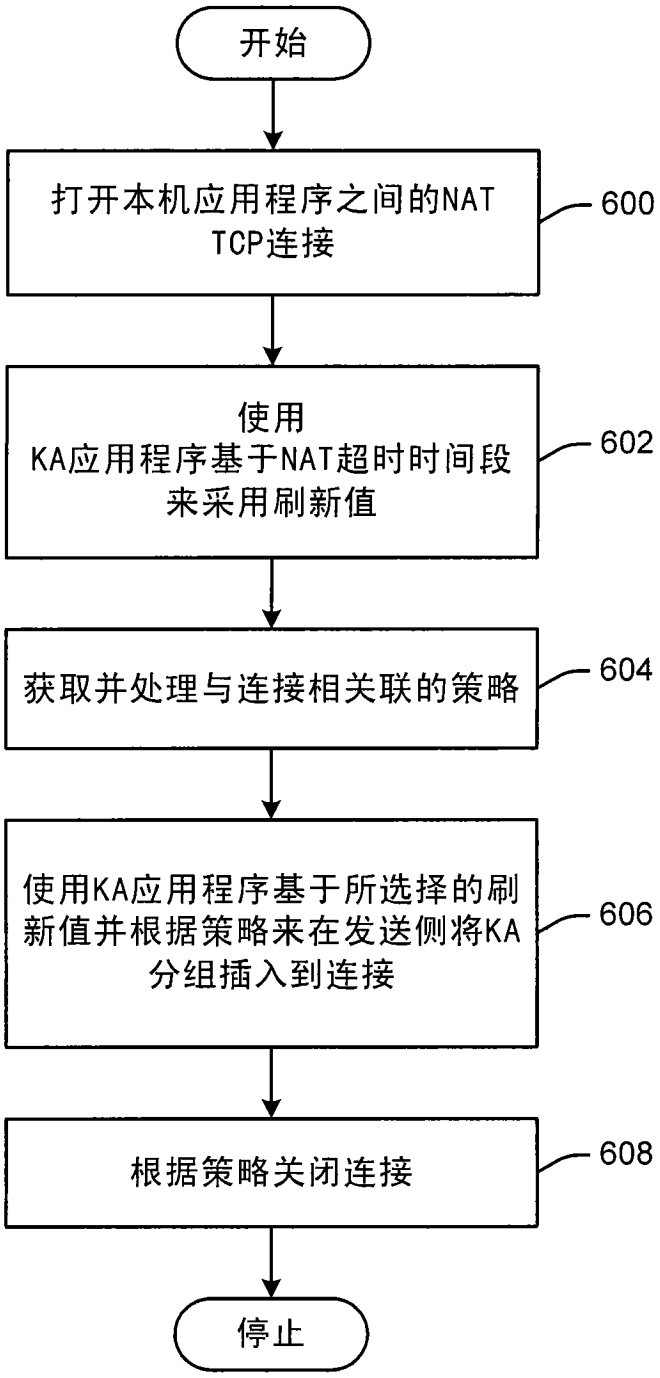

开始
打开本机应用程序之间的NAT TCP连接
600
使用 KA应用程序基于NAT超时时间段来采用刷新值
602
获取并处理与连接相关联的策略
604
使用KA应用程序基于所选择的刷新值并根据策略来在发送侧将KA分组插入到连接
606
根据策略关闭连接
608
停止

图 6

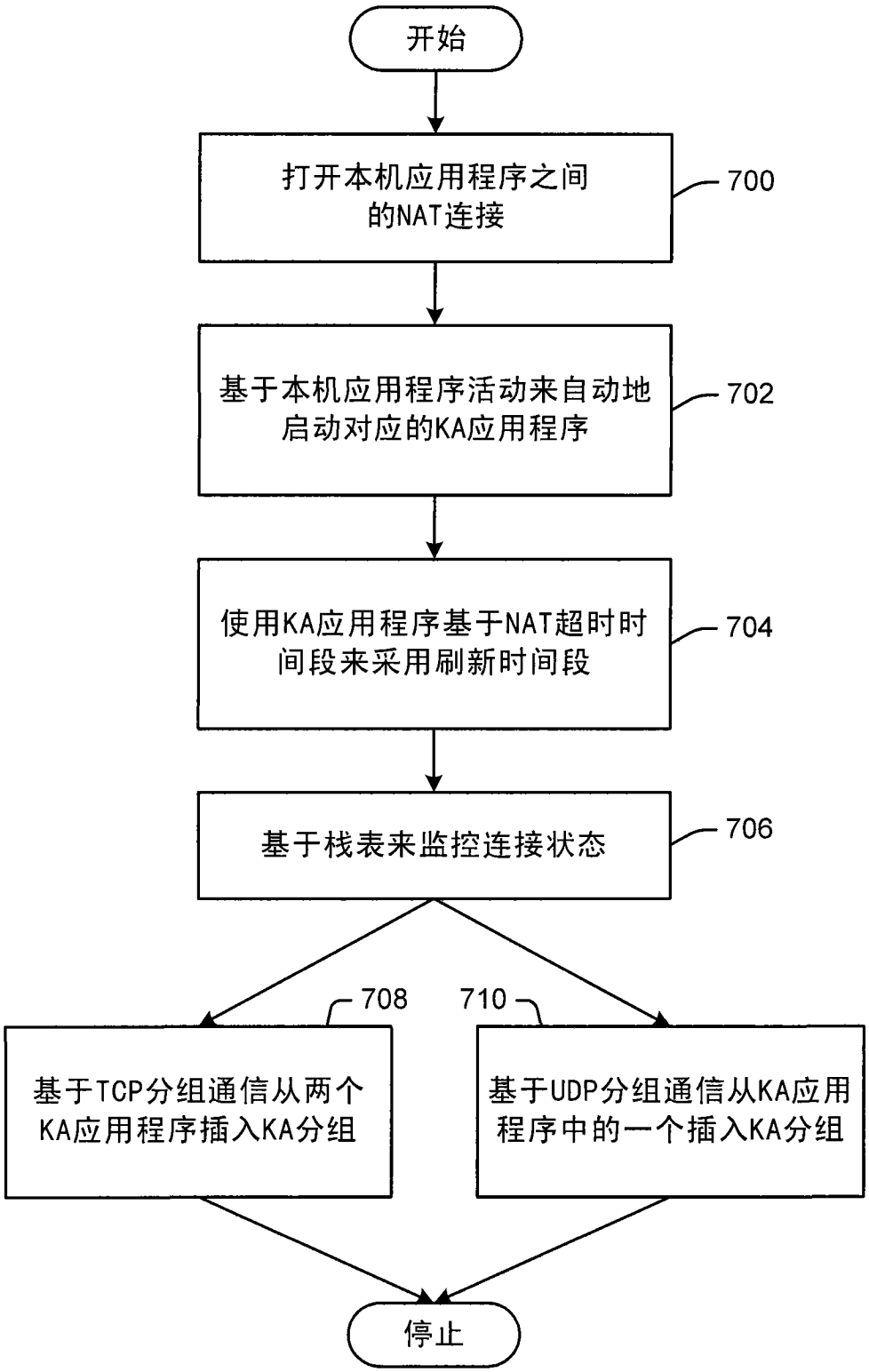

开始
打开本机应用程序之间的NAT连接
700
基于本机应用程序活动来自动地启动对应的KA应用程序
702
使用KA应用程序基于NAT超时时间段来采用刷新时间段
704
基于栈表来监控连接状态
706
708
710
基于TCP分组通信从两个KA应用程序插入KA分组
基于UDP分组通信从KA应用程序中的一个插入KA分组
停止

图 7

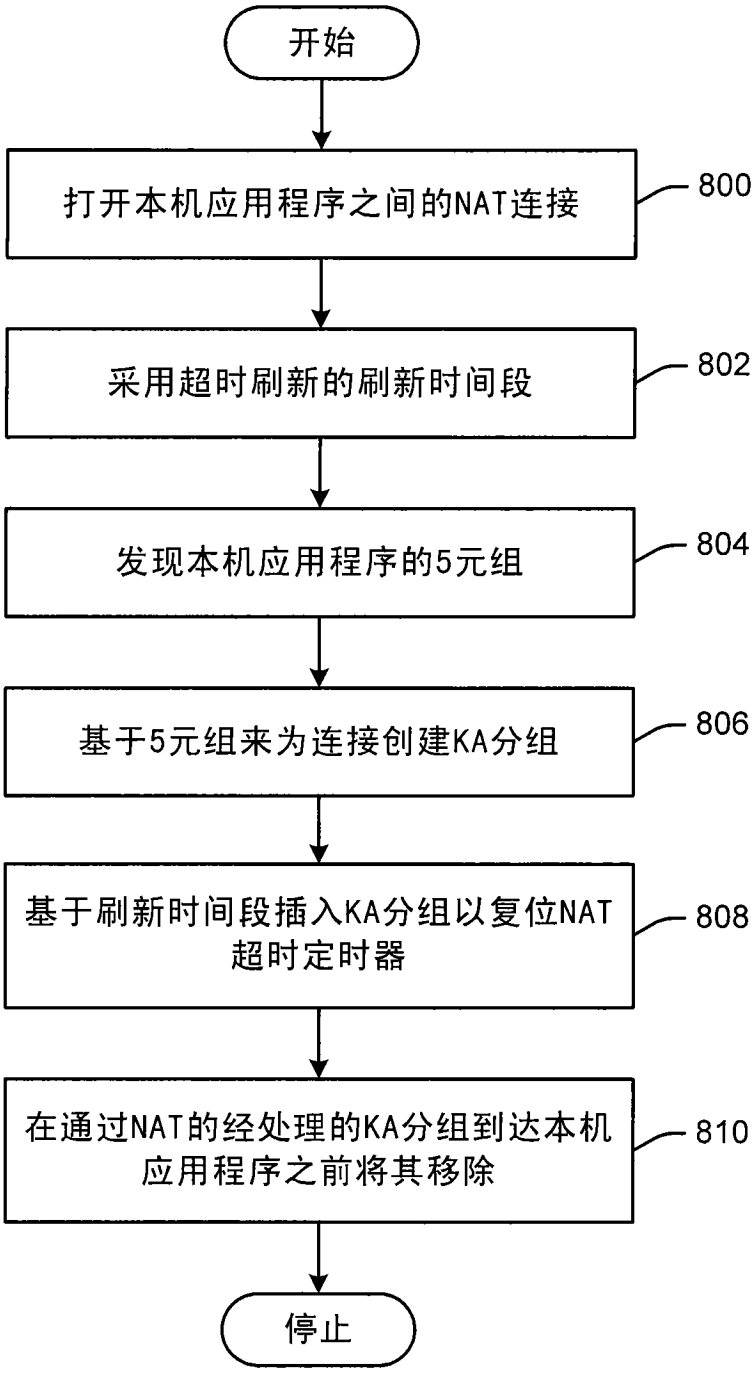

开始
打开本机应用程序之间的NAT连接
800
采用超时刷新的刷新时间段
802
发现本机应用程序的5元组
804
基于5元组来为连接创建KA分组
806
基于刷新时间段插入KA分组以复位NAT超时定时器
808
在通过NAT的经处理的KA分组到达本机应用程序之前将其移除
810
停止

图 8

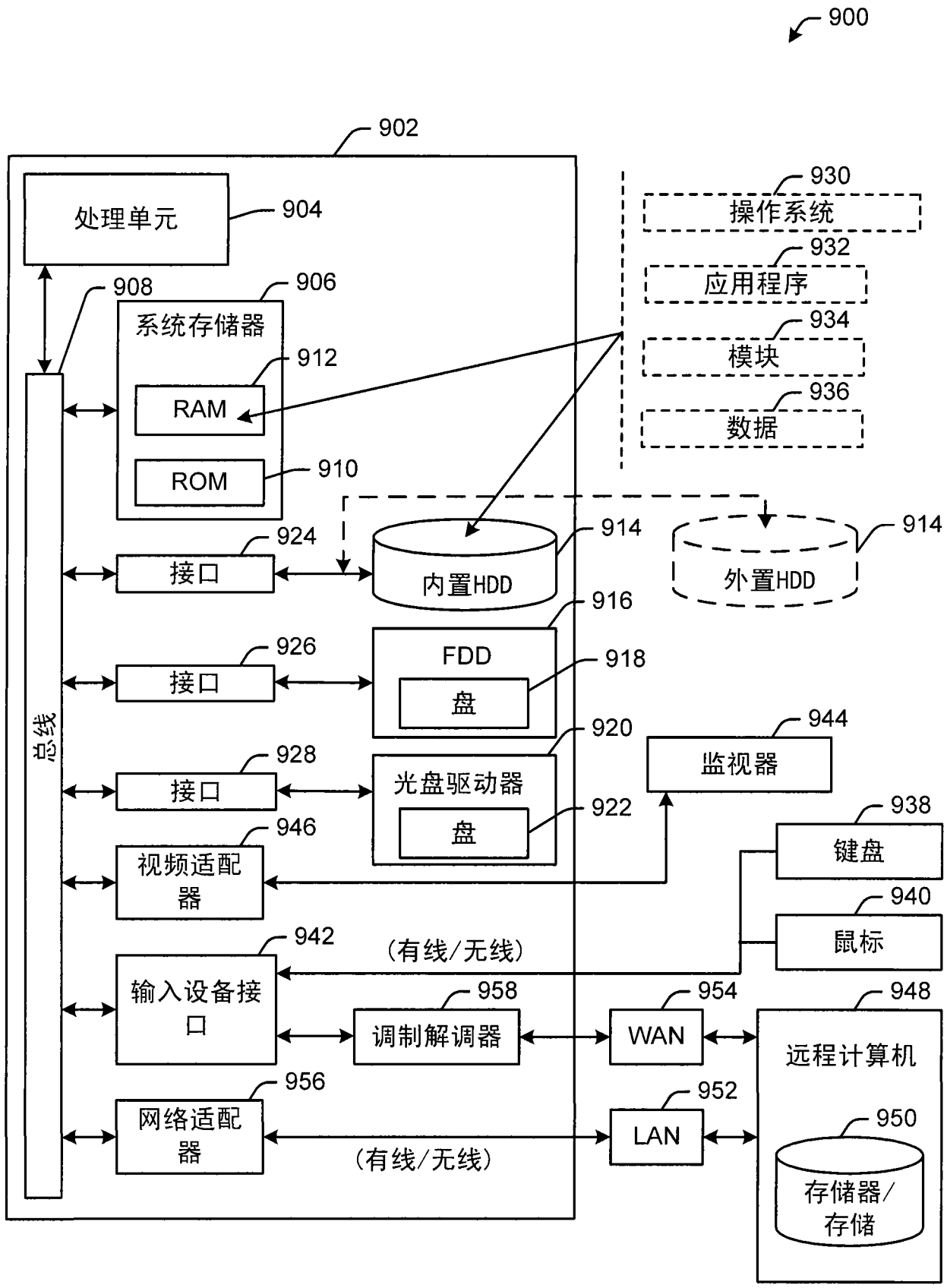

900
902
处理单元
904
908
906
系统存储器
912
RAM
ROM
910
930
操作系统
932
应用程序
934
模块
936
数据
914
内置HDD
914
外置HDD
924
接口
916
FDD
盘
926
接口
918
920
光盘驱动器
盘
928
接口
922
944
监视器
938
键盘
946
视频适配器
940
鼠标
942
(有线/无线)
输入设备接口
958
调制解调器
954
WAN
948
远程计算机
956
网络适配器
952
LAN
950
存储器/存储
(有线/无线)
总线

图 9

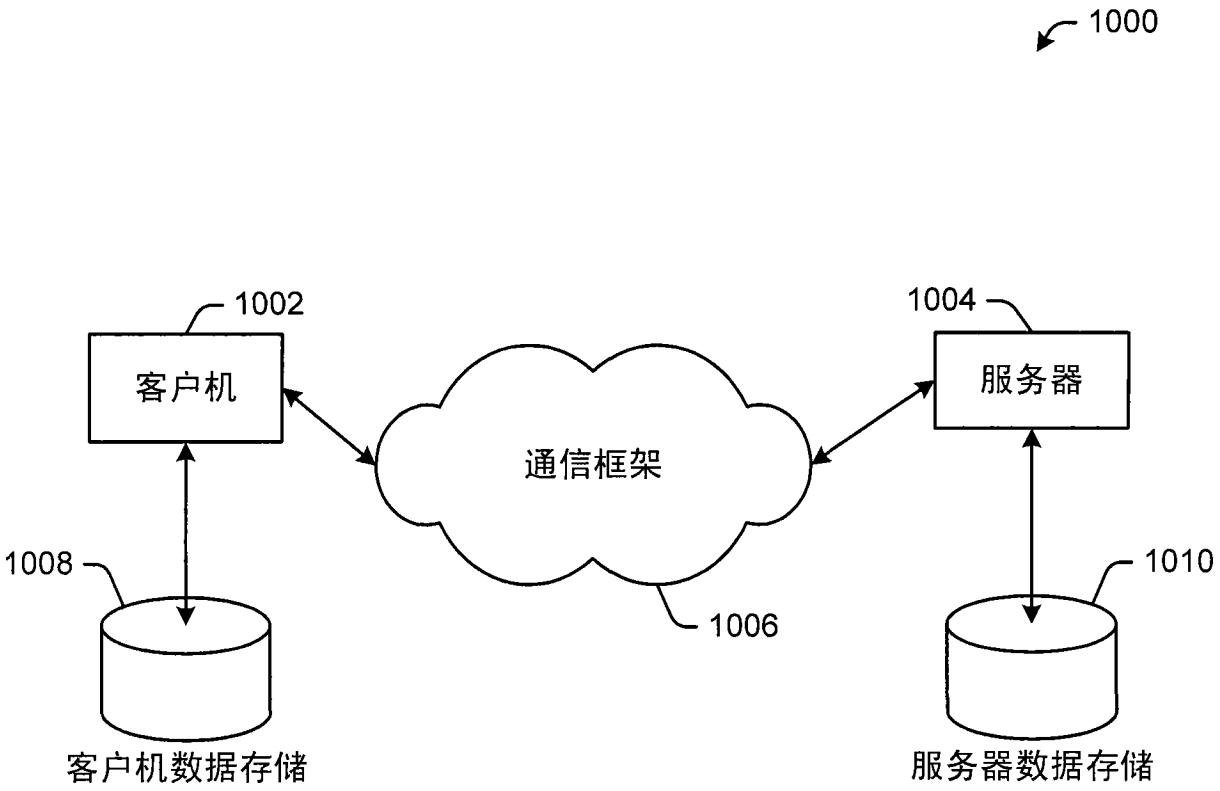


图 10