(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 1677976 B
(45)授权公告日 2011.06.08

(21)申请号 200510059096.X
(22)申请日 2005.03.21
(30)优先权数据
10/804,357 2004.03.19 US
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 P·巴尔
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 张欣
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/28(2006.01)
(56)对比文件
US 2002/0161905 A1,2002.10.31, 全文.
CN 1404277 A,2003.03.19, 全文.
CN 1473445 A,2004.02.04, 全文.
Torsten Braun, Marc Danzeisen.Secure Mobile IP Communication.local computer networks, 2001, proceedings.2001,586-593.
审查员 刘真

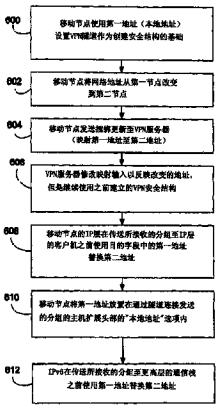
权利要求书 3 页 说明书 12 页 附图 6 页

(54)发明名称

再使用于移动计算设备的虚拟专用网络结构

(57)摘要

揭示了帮助在分配给移动节点的多个网络地址之间维持虚拟专用网络结构的方法和移动节点。该方法包括初始在移动节点和虚拟专用网络隧道服务器之间建立虚拟专用网络隧道。支持虚拟专用网络隧道的虚拟专用网络结构是基于指定用于移动节点的本地地址。当移动节点改变地址时,移动节点传送捆绑更新至指定新的网络地址的虚拟专用网络隧道服务器。此后,创建从移动节点的新的网络地址至本地地址的映射关系,因此帮助基于移动节点的本地地址继续使用虚拟专用网络结构。



CN 1677976 B

1. 一种在分配给移动节点的多个网络地址之间维持虚拟专用网络结构的方法，该方法包括：

在虚拟专用网络隧道服务器和移动节点之间设置虚拟专用网络隧道，其中支持该虚拟专用网络隧道的虚拟专用网络结构是基于用于移动节点的相对静态分配的本地网络地址的；

分配新的网络地址给移动节点，该新的网络地址不同于移动节点的本地网络地址；

由移动节点传送捆绑更新至虚拟专用网络隧道服务器以指定新网络地址；以及

创建用于移动节点的从新网络地址至本地网络地址的映射关系，由此促进基于移动节点的本地网络地址的虚拟专用网络结构的继续使用。

2. 如权利要求 1 所述的方法，其特征在于，所述虚拟专用网络结构包括安全结构。

3. 如权利要求 2 所述的方法，其特征在于，所述安全结构包括因特网安全结构。

4. 如权利要求 1 所述的方法，其特征在于，所述虚拟专用网络结构包括隧道结构。

5. 如权利要求 1 所述的方法，其特征在于，所述创建步骤包括：

由所述虚拟专用网络隧道服务器更新一映射结构以把在捆绑更新中提供的新的网络地址信息结合进来。

6. 如权利要求 1 所述的方法，还包括：在传送步骤之后，

由移动节点从虚拟专用网络隧道服务器接收包括新的网络地址的消息，以及

由移动节点以本地网络地址来替换新的网络地址。

7. 如权利要求 6 所述的方法，其特征在于，所述替换步骤由中间协议栈层执行，该层实现分组地址操作策略，所接收的消息分组之后被传送到中间协议栈层的客户机。

8. 如权利要求 7 所述的方法，其特征在于，所述中间协议栈层包括因特网协议层。

9. 如权利要求 1 所述的方法，还包括：在传送步骤之后，由移动节点把所述新网络地址置入在源地址字段中、把本地网络地址置入传送到虚拟专用网络隧道服务器的分组的扩展头部中。

10. 如权利要求 9 所述的方法，还包括下述步骤：

由虚拟专用网络隧道服务器以由移动节点传送到虚拟专用网络隧道服务器的分组的扩展头部中指定的本地网络地址来替换新的网络地址。

11. 如权利要求 10 所述的方法，其特征在于，所述替换步骤由中间协议栈层执行，该层实现分组地址操作策略，其中所接收的消息分组之后被传送到中间协议栈层的客户机。

12. 一种用于在分配给移动节点的多个网络地址之间维持虚拟专用网络结构的系统，该系统包括：

用于在虚拟专用网络隧道服务器和移动节点之间设置虚拟专用网络隧道的装置，其中支持该虚拟专用网络隧道的虚拟专用网络结构是基于用于移动节点的相对静态分配的本地网络地址的；

用于分配新的网络地址给移动节点的装置，该新的网络地址不同于移动节点的本地网络地址；

用于由移动节点传送捆绑更新至虚拟专用网络隧道服务器以指定新网络地址的装置；以及

用于创建用于移动节点的从新网络地址至本地网络地址的映射关系，由此便于基于移

动节点的本地网络地址的虚拟专用网络结构的继续使用的装置。

13. 如权利要求 12 所述的系统，其特征在于，所述虚拟专用网络结构包括安全结构。

14. 如权利要求 13 所述的系统，其特征在于，所述安全结构包括因特网安全结构。

15. 如权利要求 12 所述的系统，其特征在于，所述虚拟专用网络结构包括隧道结构。

16. 如权利要求 12 所述的系统，其特征在于，所述用于创建的装置还包括：

用于由所述虚拟专用网络隧道服务器更新一映射结构以结合进在捆绑更新中提供的新的网络地址信息的装置。

17. 如权利要求 12 所述的系统，还包括：

用于由移动节点从虚拟专用网络隧道服务器接收包括新的网络地址的消息的装置，以及

用于由移动节点以本地网络地址来替换新的网络地址的装置。

18. 如权利要求 17 所述的系统，其特征在于，所述替换步骤由中间协议栈层执行，该层实现分组地址操作策略，且其中所接收的消息分组之后被传送到中间协议栈层的客户机。

19. 如权利要求 18 所述的系统，其特征在于，所述中间协议栈层包括因特网协议层。

20. 如权利要求 12 所述的系统，还包括：

用于在在传送步骤之后，由移动节点把新网络地址置入在源地址字段中、把本地网络地址置入在传送到虚拟专用网络隧道服务器的分组的扩展头部中的装置。

21. 一种由虚拟专用网络 (VPN) 服务器实现的用于帮助在分配给移动节点的多个网络地址之间维持虚拟专用网络结构的方法，所述方法包括配置所述 VPN 服务器以执行以下步骤：

在虚拟专用网络隧道服务器和移动节点之间设置虚拟专用网络隧道，其中支持该虚拟专用网络隧道的虚拟专用网络结构是基于用于移动节点的相对静态分配的本地网络地址的；

首先从移动节点接收一对虚拟专用网络隧道服务器的捆绑更新以指定分配给该移动节点的新的网络地址，该新的网络地址不同于该移动节点的本地网络地址；以及

创建用于移动节点的从新网络地址至本地网络地址的映射关系，由此帮助基于移动节点的本地网络地址继续使用虚拟专用网络结构。

22. 如权利要求 21 所述的方法，其特征在于，所述虚拟专用网络结构包括安全结构。

23. 如权利要求 22 所述的方法，其特征在于，所述安全结构包括因特网安全结构。

24. 如权利要求 21 所述的方法，其特征在于，所述虚拟专用网络结构包括隧道结构。

25. 如权利要求 21 所述的方法，其特征在于，所述创建步骤包括：

由所述虚拟专用网络隧道服务器更新一映射结构以结合进在捆绑更新中提供的新的网络地址信息。

26. 如权利要求 21 所述的方法，其特征在于，还包括配置所述 VPN 服务器以在传送步骤之后执行进一步的步骤：

由移动节点从虚拟专用网络隧道服务器接收包括新的网络地址的消息，以及

由移动节点以本地网络地址来替换新的网络地址。

27. 如权利要求 26 所述的方法，其特征在于，所述替换步骤由中间协议栈层执行，该层实现分组地址操作策略，且其中所接收的消息分组之后被传送到中间协议栈层的客户机。

28. 如权利要求 27 所述的方法，其特征在于，所述中间协议栈层包括因特网协议层。

再使用于移动计算设备的虚拟专用网络结构

技术领域

[0001] 本发明一般涉及计算机系统领域。更具体地说，本发明关于用于维持移动网络节点的网络连接性的方法和系统。移动网络节点包括，例如，具有无线网络通信接口的便携式计算设备。更确切地说，本发明是针对确保在移动节点的当前分配的物理网络（即，因特网协议）地址改变后网络中的其他节点仍然可以与该节点通信的方法和系统。

[0002] 背景技术

[0003] 移动网络服务在便携式设备由用户携带至不同的地点时帮助将便携式计算设备，一般是临时地，连接至多个网络中的任何一个。这种能力通常，尽管不是总是和无线WAN/LAN连接相关。例如，一笔记本电脑可通过多个在地理上位于分散的位置的无线热点(hotspot)连接至一网络（或者其子网络）。当一便携式设备连接到一个这样的子网络时，该便携式设备接收唯一的网络（即，因特网协议）地址。移动计算的一方面是使其他节点保持维持接入到一移动节点的通信的能力，尽管实际上是接入到一使用不同于永久的“本地”地址的当前地址的网络。因此，开发了一些机制来适应在一些地点，移动节点的网络地址会发生改变的实际可能性，且之后其他节点将会以其新的网络地址试图与该移动节点通信。

[0004] 在描述一种先前的公知的网络操作移动节点网络地址改变的方法之前，示例的相关网络协议将会被简要地描述。多种网络协议支持为便携式计算设备建立临时连接并为这些计算设备分配网络地址。一种公知的动态主机配置协议(DHCP)能在连接到一网络时集中地、自动地将因特网协议地址分配给机器。DHCP使得计算机能够移动到网络中的另一个位置并自动地接收和新位置相对应的新的因特网协议地址。DHCP并入了网络地址的“租用”功能，其会分配可变量的时间，在这段时间内一特定分配的因特网协议地址可有效用于连接计算机。DHCP在仅有有限数量的因特网协议地址可用于分配给大量计算机的网络环境中尤其有用。

[0005] 点对点协议(PPP)是一种用于两台计算机之间的串行通信的通信协议（例如，个人计算机通过电话线连接至服务器）。PPP使用因特网协议并提供数据链路层（第二层）服务。具体地说，PPP压缩TCP/IP或者其他网络层协议分组并将如同从客户机网关传送到因特网般地将它们从客户机传送到服务器。

[0006] 和移动计算潜在相关的其他协议包括点对点隧道协议(PPTP)和第二层隧道协议(L2TP)。PPTP是PPP的扩展，其帮助网络通过公共网络（例如，因特网）上的专用的“隧道”进行扩展。这种形式的互联称为虚拟专用网络(VPN)，其使得具有PPP客户机支持的计算机能够通过因特网服务提供者建立至服务器的安全连接。L2PT是PPTP的一种变化。这两个隧道协议都使用本地接入集中器(concentrator)来使得分组可在公共网络链接中用隧道传输(tunneled)，从而避免建立长距离电话连接以保证客户机和服务器之间的安全通信的潜在需求。

[0007] 在一种公知的网络环境中，移动计算设备被分配一和“本地”网络位置关联的相对永久的网络地址。然而，当移动节点从其本地网络之外的位置连接时，一网络通信服务器，例如使用DHCP来分配临时的当前地址给移动节点以支持在本地网络位置以外的连接。在

移动节点使用临时地址而不是其本地地址期间，相应的节点（即，其他试图与移动节点进行通信的节点）将使用之前被提供给该移动节点的地址。通常，除非通知了移动节点的当前的、非本地的地址，对应的节点在发送分组至移动节点时使用移动节点的本地（永久地址）。如果移动节点在不同于其本地位置的网络位置连接，本地地址和移动节点的当前地址不匹配。在公知的网络安排中，这种情况通过在移动节点的本地网络上提供移动节点的本地代理来解决。本地代理维持具有特定本地网络地址的移动节点的当前地址。本地代理接收指向移动节点的本地网络地址的分组、按照隧道协议压缩分组、并将压缩后的分组传送到移动节点的当前地址。外壳 (envelope) 的“来”和“去”地址分别标识了本地代理和节点附件的临时当前点，而所压缩的分组标识了所接收的分组的原本的源和目的地址。

[0008] 下面说明公知的基于本地代理的移动网络安排的操作。据有本地地址为 1111 的移动节点当前通过临时分配的为 2222 的非本地地址远程连接到其本地网络。具有本地地址为 7777 的对应节点使用为 1111 的本地地址来与移动节点通信。本地代理（具有地址 1110）感觉到的移动节点的当前非本地地址为 2222，拦截识别移动节点的本地地址 (1111) 的分组。本地代理按照一隧道协议压缩指向本地地址 1111 的分组。压缩后的分组指定了本地代理源地址 (1110) 和移动节点当前地址 (2222)。

[0009] 本地代理解决在移动网络环境中出现的许多网络地址跟踪问题。例如，如果对应的节点和移动节点同时移动，由每个节点提供的关于该节点的最新已知地址的捆绑更新会丢失。如果这两个节点参加到一个会话中，该会话会由于正确地址的丢失而不能继续。换句话说，如果存在用于这两个节点的本地代理，则两个节点可使用用于这些节点的本地代理来继续通信。本地代理拦截并传送（用隧道传输）标识本地地址的分组至用于移动和对应节点的当前（“转接 (care of)”）地址。

[0010] 关于移动节点的另一个会出现的潜在的地址跟踪问题涉及，在用于将名字和网络地址相关的域名系统 (DNS) 服务器已经缓存了和移动节点相关的名称的旧地址时，新节点联系该移动节点的能力。在这种情况下，DNS 服务器，或者更一般地说名称服务器 (name server) 继续提供旧的 / 无效的地址直到该缓存的用于已命名的移动节点的地址的生存时间终止为止 (TTL)。本地代理通过拦截包含由 DNS 服务器向新节点提供的移动节点的（本地）地址的分组（并之后用隧道传输至移动节点）来解决这个问题。当移动节点接收用隧道传输的分组时，可通过捆绑更新通知新节点关于其新的地址（本地代理之后被绕过）。

[0011] 另一个地址跟踪问题涉及移动在网络地址传送器 / 防火墙之后的移动节点。在这种情况下用隧道传输本地代理从新客户机至该移动节点的业务。本地代理具有用于与移动节点进行通信的开放端口，作为之前由移动节点从 NAT/ 防火墙后面起始的至本地代理的通信的结果。新的客户机使用已知的移动节点的本地地址非直接地与移动节点通信（通过本地代理）。当管理网络地址 / 通信的复杂度增加时，本地代理被视为充满移动节点的网络环境中有价值的，即使不是不可或缺的组件。

[0012] 另外一个涉及移动节点的挑战是在建立了虚拟专用网络隧道至其本地网或之后且仍然处于其本地网络之外时移动节点改变地址的可能性。新的地址会使得之前建立的虚拟专用网络隧道结构废弃。在这种情况下，新的隧道和相关的结构，包括网络安全结构在每一次网络地址改变时被建立。在高度移动网络节点的情况下，这种瓦解严重削弱用户的整体经历。

发明内容

[0013] 本发明包括解决上述的在移动节点被分配新的网络地址时出现的问题的方法和网络管理框架。具体地说，本发明包括由移动节点执行的方法，其在分配给移动节点的多个网络地址上维持虚拟专用网络结构。起始时，虚拟专用网络隧道在移动节点和虚拟专用网络隧道服务器之间建立。支持虚拟专用网络隧道的虚拟专用网络结构是基于指定用于该移动节点的本地地址 (home address)。此后，该移动站被分配一新的网络地址。新的网络地址不同于用于该节点的本地地址。

[0014] 移动节点通过传送一指定新的网络地址的捆绑更新至虚拟专用网络隧道服务器来通知虚拟专用网络隧道服务器关于其新的网络地址。建立从移动节点的新的网络地址至本地地址的映射关系。该映射关系，以及网络通信协议栈的较低层中的替代逻辑一起帮助继续使用基于移动节点的本地地址的虚拟专用网络结构。

[0015] 本发明还记载在移动节点或者计算机可执行的指令中，其结合了上述的映射功能。此外，按照本发明的具体实施例，对于虚拟专用网络结构的再使用可采取各种不同的形式，包括安全结构和隧道结构。

[0016] 此外，本发明的实施例中，方法还包括 VPN 服务器更新映射结构以使移动节点的新地址被映射到将被用于使用再使用的隧道数据结构执行特定的安全以及隧道操作的本地地址。移动节点还维持这些映射的地址关系。如此，在本地地址和新的网络地址之间建立了映射关系之后，一旦移动节点从虚拟专用网络隧道服务器接收包括新网络地址的消息，移动节点使用所接收的消息分组的目的地字段中的本地地址来替换新的网络地址。在本发明的一 个实施例中，该替换在 TCP/IP 协议栈的中间（例如，IP- 因特网协议）层被执行。此外，这些替换在反向消息传输方向上由虚拟专用网络隧道服务器在从移动节点接收的分组上实现（基于在所接收的消息的扩展中所提供的本地地址）。

附图说明

[0017] 所附的权利要求具体说明了本发明的特征，本发明以及其目标和优势可以从下列结合附图的详细描述中得到最佳的理解，其中，

[0018] 图 1 是说明用于实现本发明的实施例的计算设备的示例架构的简化示意图；

[0019] 图 2 是一示例网络环境，其中一个或多个移动节点通过多种远程位置中的任何一个可通信地连接到本地网络并接收不同于相对静态分配给本地网络中的移动节点的本地地址的动态分配的地址；

[0020] 图 3 概述了用于适用于实现本发明的网络化节点的示例通信栈；

[0021] 图 4 概述了由移动节点执行的用于以不同于分配给该移动节点的之前的网络地址的地址连接至一非本地网络的一组步骤；

[0022] 图 5 概述了响应于两个节点在基本上相同的时间移动到新的网络位置时，在一组网络节点和与它们相关的授权名称服务器之间传送的通信，以及；

[0023] 图 6 概述了当移动节点移动到不同的外部网络地址时，一组被执行以实现再使用虚拟专用节点和其相关结构的步骤。

[0024] 附图详述

[0025] 此处揭示了一种用于支持与移动网络节点相关的变化地址的方法和框架。这种支持通过下列步骤而被提供：对移动网络节点的增强和使用 DNS 动态主机配置协议 (DHCP)，以及虚拟专用网络 (VPN) 服务器（或者它们的功能等价体）来动态分配一当前网络地址至一移动节点，提供当前网络地址至授权名称服务器，并之后使相应的节点基于由授权名称服务器所提供的地址升级它们的用于移动节点的地址——相对于在复制的名称服务器中缓存的地址。

[0026] 更具体地说，移动节点在其授权 DNS 服务器上使用为 0 的生存时间注册其所有的名称 -- 地址映射。将生存时间指定为 0 保证了非授权的（缓存 / 复制）DNS 服务器或者客户机上的 DNS 名称解析器不会在其缓存中保存名称 / 地址的组合。因此，当对应的节点由于移动节点位置的改变丢失对于移动节点的当前地址的跟踪时，对应的节点将依靠保存在非授权 DNS 服务器或者其自己的名称解析器缓存中的旧地址。

[0027] 所说明的本发明的实施例的第二个方面包括配置移动节点来启动一至安全区域中的虚拟专用节点服务器的虚拟专用网络连接，当移动节点从该安全区域以外建立连接时，移动节点与该服务器相关联。移动节点在起始注册到其本地安全区域之外的新网络（以及在该新网络上接收新的地址配置）之后，通过其本地安全区域中的 VPN 服务器建立一用隧道传输的连接至其本地安全区域。VPN 服务器在本地安全区域中为该移动节点建立一新的地址。该新的地址保存在授权 DNS 服务器中用于本地安全区域（生存时间为 0）。当使用之前的用于该移动节点的地址注册失败时，相应节点的获得由授权 DNS 服务器提供的新地址来通过该由该 VPN 服务器支持的用隧道传输的连接与该移动节点通信。在安全区域是公共的情况下，即网络上的机器可以直接接入到其他网络上的其他机器，建立虚拟专用网络连接时不必要的。

[0028] 此外，在所说明的本发明的实施例中，当移动节点移动到新的外部网络地址时，之前建立的 VPN 隧道被再使用。这种功能通过使用在移动因特网协议分组中支持的扩展头部和发布至一负责 VPN 服务器的捆绑更新来协助，该更新用于映射当前外部转接 (care of) 网络地址至形成用于按照 VPN 隧道再使用所维持的结构的基础用户移动节点的本地地址。因此，在初始设置了 VPN 隧道和其相关的结构之后，当移动节点接收新的外部转接网络地址时，该结构被维持。

[0029] 图 1 图示地说明了用于在由多个、可通信地耦合的网络所支持的环境中使用的移动计算设备（例如，笔记本或者平板电脑）的合适的操作环境 100 的示例，其中该移动计算设备能够连接到这些网络。计算系统环境 100 仅为合适的计算环境的一个示例，并非暗示对本发明的使用范围或功能的局限。本发明可以使用众多其它通用或专用计算系统环境或配置来操作。适合使用本发明的众所周知的计算系统、环境和 / 或配置包括但不限于：个人计算机、服务器计算机、手持式或膝上设备、平板设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费者电子设备、网络 PC、小型机、大型机、包括任一上述系统或设备的分布式计算环境等等。

[0030] 本发明将在诸如由网络环境中的计算机执行的程序模块等计算机可执行指令的一般上下文环境中描述。一般而言，程序模块包括例程、程序、对象、组件、数据结构等等，执行特定的任务或实现特定的抽象数据类型。本发明潜在地可被结合于在分布式计算环境中操作的网络节点，在分布式网络环境中，任务由通过一通信网络相链接的远程处理设备执

行。在分布式网络环境中，程序模块一般位于本地以及 / 或者包括存储储存设备的远程计算机存储媒质中。

[0031] 继续参考图 4，用于实现本发明的示例系统包括以常规计算机形式 110 的通用计算装置。计算机 110 的组件，但不限于处理单元 120、系统存储器 130 以及将包括系统存储器耦合至处理单元 120 的系统总线 121。系统总线 121 可以是若干种总线结构类型的任一种，包括存储器总线或存储器控制器、外围总线以及使用各类总线体系结构的局部总线。作为示例而非局限，这类体系结构包括工业标准体系结构 (ISA) 总线、微通道体系结构 (MCA) 总线、增强 ISA(EISA) 总线、视频电子技术标准协会 (VESA) 局部总线以及外围部件互连 (PCI) 总线，也称为 Mezzanine 总线。

[0032] 计算机 110 通常包括各种计算机可读媒质。计算机可读媒质可以是可由计算机 110 访问的任一可用媒质，包括易失和非易失媒质、可移动和不可移动媒质。作为示例而非局限，计算机可读媒质包括计算机存储媒质和通信媒质。计算机存储媒质包括以用于储存诸如计算机可读指令、数据结构、程序模块或其它数据等信息的任一方法或技术实现的易失和非易失，可移动和不可移动媒质。计算机存储媒质包括但不限于，RAM、ROM、EEPROM、闪存或其它存储器技术、CD-ROM、数字多功能盘 (DVD) 或其它光盘存储、磁盒、磁带、磁盘存储或其它磁存储设备、或可以用来储存所期望的信息并可由计算机 110 访问的任一其它媒质。通信媒质通常在诸如载波或其它传输机制的已调制数据信号中包含计算机可读指令、数据结构、程序模块或其它数据，并包括任一信息传送媒质。术语“已调制数据信号”指以对信号中的信息进行编码的方式设置或改变 其一个或多个特征的信号。作为示例而非局限，通信媒质包括有线媒质，如有线网络或直接连线连接，以及无线媒质，如声学、RF、红外和其它无线媒质，例如无线 PAN、无线 LAN 以及无线 WAN 媒质。上述任一的组合也应当包括在计算机可读媒质的范围之内。

[0033] 系统存储器 130 包括以易失和 / 或非易失存储器形式的计算机存储媒质，如只读存储器 (ROM)131 和随机存取存储器 (RAM)132。基本输入 / 输出系统 133(BIOS) 包括如在启动时帮助在计算机 110 内的元件之间传输信息的基本例程，通常储存在 ROM 131 中。RAM 132 通常包含处理单元 120 立即可访问或者当前正在操作的数据和 / 或程序模块。作为示例而非局限，图 1 示出了操作系统 134、应用程序 135、其它程序模块 136 和程序数据 137。

[0034] 计算机 110 也可包括其它可移动 / 不可移动、易失 / 非易失计算机存储媒质。仅作示例，图 1 示出了对不可移动、非易失磁媒质进行读写的硬盘驱动器 141、对可移动、非易失磁盘 152 进行读写的磁盘驱动器 151 以及对可移动、非易失光盘 156，如 CD ROM 或其它光媒质进行读写的光盘驱动器 155。可以在示例性操作环境中使用的其它可移动 / 不可移动、易失 / 非易失计算机存储媒质包括但不限于，磁带盒、闪存卡、数字多功能盘、数字视频带、固态 RAM、固态 ROM 等等。硬盘驱动器 141 通常通过不可移动存储器接口，如接口 140 连接到系统总线 121，磁盘驱动器 151 和光盘驱动器 155 通常通过可移动存储器接口，如接口 150 连接到系统总线 121。

[0035] 图 1 讨论并示出的驱动器及其关联的计算机存储媒质为计算机 110 提供了计算机可读指令、数据结构、程序模块和其它数据的存储。例如，在图 1 中，示出硬盘驱动器 141 储存操作系统 144、应用程序 145、其它程序模块 146 和程序数据 147。注意，这些组件可以与操作系统 134、应用程序 135、其它程序模块 136 和程序数据 137 相同，也可以与它们不同。

这里对操作系统 144、应用程序 145、其它程序模块 146 和程序数据 147 给予不同的标号来说明至少它们是不同的副本。用户可以通过输入设备，如输入板或电子数字化仪 164、麦克风 163、键盘 162 和定位设备 161（通常指鼠标、跟踪球或触摸板）向计算机 110 输入命令和信息。其它输入设备（未示出）可包括操纵杆、游戏垫、圆盘式卫星天线、扫描仪等等。这些和其它输入设备通常通过耦合至系统总线的用 户输入接口 160 连接至处理单元 120，但是也可以通过其它接口和总线结构连接，如并行端口、游戏端口或通用串行总线 (USB)。监视器 191 或其它类型的显示设备也通过接口，如视频接口 190 连接至系统总线 121。监视器 191 也可以与触摸屏面板或其类似物组合。注意，监视器和 / 或触摸屏面板可以物理地耦合至结合计算设备 110 的外壳，如平板类型的个人计算机。另外，诸如计算设备 110 的计算机也包括其它外围输出设备，如扬声器 197 和打印机 196，通过输出外围接口 194 或其类似物连接。

[0036] 计算机 110 可以在使用到一个或多个远程计算机，如远程计算机 180 的逻辑连接的网络化环境中操作。远程计算机 180 可以是个人计算机、服务器、路由器、网络 PC、对等设备或其它公用网络节点，并通常包括许多或所有上述与计算机 110 相关的元件，尽管在图 1 中仅示出了存储器存储设备 181。图 1 描述的逻辑连接包括局域网 (LAN)171 和广域网 (WAN)172，这里示出作为示例而非局限。这类网络环境常见于办公室范围或企业范围计算机网络、内联网以及因特网。

[0037] 当在局域网网络环境中使用时，计算机 110 通过网络接口或适配器 170 连接至局域网 171。此外，一个或多个有线 / 无线网络接口 170 的组支持在 WAN 173 上的通信。虽然没有在图 1 中示出，计算机 110 可潜在地包括内置的或者外置的调制解调器，通过用户输入接口 160 或者其他合适的机制连接到系统总线 121。在网络化环境中，描述的与计算机 110 相关的程序模块或其部分可储存在远程存储器存储设备中。为了示例而不是限制，图 1 示出了远程应用程序驻留在存储设备 181 上。可以理解，示出的网络连接是示例性的，也可以使用在计算机之间建立通信链路的其它装置。

[0038] 在描述其中可以具有优势地结合本发明的示例网络环境之前，用于描述本发明的实施例的术语将首先被提供。一般，本发明在一网络环境中实现，包括企业网（即，有公司维护的网络），这种网络一般由包括一个或多个虚拟专用网络 (VPN) 服务器集成在内的防火墙保护。因此，用户可以通过初始连接到公共和本地网络（即，在本地网络中的）并之后建立一至企业网的 VPN 隧道来接入连接到企业网的资源 / 实体。

[0039] “安全区域”是接入至 / 来自在一些其他形式中限制（例如，要求通过注册 过程对用户进行识别 / 授权）的区域的互连性的最小区域。安全区域的例子包括由防火墙 /NAT 保护的本地网络、由周围 (perimeter) 防火墙保护的企业网络、以及诸如因特网的未保护的公共网络，其中的接入是不受保护的，但是其区域宽度 (domain breadth) 通过由所连接的其他安全区域所建立的周围防火墙定界 (delimited)。

[0040] “移动区域”是节点区域，其中与该节点建立的会话在节点在一个或者多个安全区域中以及 / 或者之间移动时保持不变。移动区域潜在地扩展了多个安全区域。

[0041] 参考图 2，说明了其中可以潜在地实现本发明的网络计算环境的简单示例。在所示出的环境中，以几乎是任何便携式计算设备（例如，笔记本或者平板计算机、PDA、智能电话等等）的形式出现的移动节点 200 包括一个或多个网络接口（没有专门示出），这些网络

接口帮助通过多种网络接口技术连接至多个网络。在图 2 说明的特定实施例中，移动节点 200 潜在地通过的无线收发机 204（通过 802 11a/b/g 媒体规则 / 协议）通信，该无线收发机可通信地耦合至对应于移动节点 200 的本地网络的局域网 206。无线收发机 204（也称为无线接入点或者 WAP）提供对于 LAN 206 上的多种资源的接入。例如，无线收发机 204 提供笔记本计算机 200 接入至在文件服务器 208 和由 DNS 服务器 209 支持的名称服务器所维持的目录。

[0042] 移动节点 200 和 214，如它们的名称所表明的，能够移动并在不同于它们的本地网络的网络上建立新的网络地址（与以太网链接 206 相关）。在图 2 说明的示例性移动网络环境中，当位于它们的本地网络之外时，移动节点 200 和 214 通过包括蜂窝传输塔 202 的蜂窝传输网络接入到多个网络 / 资源，包括相互接入。在图 2 说明的移动网络环境中，移动节点 200 和 214 通过提供第一跳跃 (hop) 连接至一连接至因特网 212 的蜂窝网络的蜂窝传输塔 202 与连接至其他网络，包括 LAN 206 的实体（直接或者间接地）相连接。当移动节点 200 和 214 位于它们的本地网络（即，LAN 206）之外时，包括 / 相关于一虚拟专用网络 (VPN) 服务器的网关 / 防火墙 / 调制解调器 210 支持因特网 212 和连接至 LAN 206 的计算设备之间的通信。VPN 服务器组件允许通过要求外部节点建立 VPN 隧道来授权在 LAN 206 的周围 (perimeter) 的网络业务。如果没有 VPN 服务器，网关 / 防火墙 / 调制解调器 210 在许多情况下会接收对于从位于防火墙之后的实体发布的请求的响应。网关 / 防火墙 / 调制解调器 210 还提供因特网 212 的用户接入至 LAN 206 上的资源。

[0043] 在移动节点 200 和 214 上执行的应用程序潜在地建立网络连接并以对等安排的形式与静态连接的客户机节点 211（例如，桌面 PC）以及其他移动节点通过无线收发机 204 和蜂窝传输塔 202 通信。DNS 服务器 209 通过提供命名的网络实体的当前地址来支持这种对等连接。DNS 209 服务器为命名的网络实体维持一对应的地址（即，命名的网络实体在本地网络上的地址）。对于移动节点，诸如节点 200 和 214，当移动节点当前没有连接至其本地网络时，当前地址潜在地与本地地址不同。作为示例，移动节点 200 被分配了本地地址 1111，移动节点 214 被分配了本地地址 1112。当移动节点 200 和 214 连接至另一个网络时。它们接收不同于它们所分配的本地地址的网络地址。

[0044] DNS 服务器 209 响应于由试图与命名的实体建立 / 重新建立连接的网络实体提交的名称请求，为命名的网络实体，包括移动节点提供当前地址。此外，由 DNS 服务器，例如 DNS 服务器 209 使用的名称 / 地址相关表可被复制以改善对于多个 DNS 服务器的接入，一个这样的服务器被指定为对于给定网络实体的“授权”。

[0045] 当移动节点移动到新的网络地址时，由非授权 DNS 服务器在名称缓存中维持的移动节点（例如，移动节点 200 和 214）的当前地址可能临时地变得不正确。不正确的地址保留在名称缓存中直到其被更新的地址所替换，替换是由于 DNS 服务器之间可能存在的复制或者其生存时间 (TTL) 变成 0。结果，当移动节点改变地址时，与在对应的网络节点上执行的应用程序的会话会丢失 / 瓦解直到新的移动节点的新的地址被发现并放置 (bound) 到栈中。在对等连接的两个节点都是移动节点（例如，节点 200 和 214）且两个移动节点在基本相同的时间释放它们的本地网络（并因此丢失对授权 DNS 服务器的接入）的情况下，重新发现的过程会变得更加复杂。

[0046] 参考图 3，示例协议栈 300 被示意性地说明用于实现本发明的移动节点 200。示出

的协议栈 300 包括，在物理层网络接口卡 (NIC)310 通过移动节点 200 上的物理接口发送并接收通信。NIC 310 通过网络驱动器接口 320（例如，NDIS） 与协议栈 300 的上层通信。这种上层中的一种包括 VPN/ 隧道驱动器 330。VPN/ 隧道驱动器 330 支持移动节点 200 和 VPN 服务器之间的隧道连接。VPN/ 隧道驱动器 330 将消息压缩到合适的外壳中，识别在节点 200 的本地安全区域的安全区域之外的非本地地址。当移动节点不使用 VPN/ 隧道功能来在其本地网络 (LAN 206) 上通信的时，VPN/ 隧道驱动器 330 被绕过。在图 3 示出的实施例中，NDIS 320 被示为弯曲了隧道驱动器 330 的一部分，因为其被 VPN/ 隧道驱动器 330 用于连接 NIC 310 和 TCP/IP 层 340 两者。

[0047] 在示例实施例中 --TCP/IP 层 340（也包括 UDP 驱动器功能）位于 VPN/ 隧道驱动器 330 之上或者之下，为了反映这个，在示出的实施例中，VPN/ 隧道驱动器 330 即是客户机也是由 TCP/IP 层 340 调用的驱动器。TCP/IP 层 340 实现公知的传输层操作。在本发明的一个实施例中，TCP/IP 层 340 包括按条件执行的进程，以使如果响应于捆绑更新（当移动节点 200 接收新的网络地址），没有确认从再定位的移动对应节点接收，则 TCP/IP 层 340 发布一针对相应的节点的名称查询以获得最新的可用网络地址，该地址是来自移动节点的栈被配置成要进行查询的 DNS 服务器。

[0048] 一名称注册客户机 350，在示例实施例中其是移动节点 200 的动态主机配置协议 (DHCP) 客户机的一部分，包括一功能性改变以保证在从授权 DNS 服务器 209 到 (leaf)DNS 服务器获取改变的网络地址时的传播时延不会影响相应的节点从 leafDNS 服务器接收过时的信息。在一个特定实施例中，操作用于建立一本地网络安全区域中的移动节点 200 的网络地址的名称注册服务器 350 使用更加直接的方式 (further directive) 提供当前地址至其授权 DNS 服务器 209，叶 (leaf)DNS 服务器不在它们的名称缓存中保存移动节点的名称 / 地址组合。在本发明的特定实施例中，这些功能由名称注册客户机 350 实现，其向授权 DNS 服务器 209 提供具有生存时间为 0 的名称 / 网络地址更新。非授权 DNS 服务器不会缓存来自授权 DNS 服务器的地址解析响应，其中该响应指定了 TTL 为 0。结果，所有的用于移动节点 200 的名称请求唯一地参考由授权 DNS 服务器 209 维持的名称 / 地址解析信息而被解析。为了说明简单 (scalability)，仅仅一个移动节点将包括 TTL 为 0 的功能。这种移动性可通过检测一起始的装置而实现自动化，该装置检测节点是否是配置成移动的（例如，启用了电池功率和 DHCP）。

[0049] 图 3 中最后一个被识别的组件是 VPN 客户机 360。在示出的本发明的实施例中，VPN 客户机 360 起始建立一与驻留在不同于移动节点当前驻留的区域的安全区域中的 VPN 服务器的 VPN 隧道连接。在本发明的其他实施例中，没有 VPN 服务器出现在移动客户机的本地网络上。在这种情况下，移动节点通过公知的“集合 (rendezvous)”服务器建立链路回到由防火墙保护的 LAN 206。该集合服务器驻留在 LAN 206 外并可由移动节点接入。集合服务器维持至 LAN206 中的节点的恒定连接并使用该连接来通知位于 LAN 206 的防火墙的另一侧的节点，移动节点 200 试图与该节点建立连接。

[0050] 转到图 4，概述了一组有移动节点（例如移动节点 200）执行的用于再建立至对应节点，例如移动节点 214 的连接的示例步骤，上述的连接由于移动节点 200 将其位置从网络地址 (1111) 改变到和其他网络相关的网络地址，例如通过传输塔 202 接入的蜂窝网络。移动节点 200 之前将其本地地址直接提供给其授权 DNS 服务器 209 以使得该地址不需要被缓

存在非授权的DNS服务器中（例如，指定TTL为0）。还假设没有用于移动节点200的本地代理存在。在示出的示例中，在移动节点200从LAN 206解除连接之后，移动节点200通过网关/防火墙/调制解调器210从其在蜂窝网络上的新地址建立VPN隧道连接至其本地网络LAN 206。

[0051] 起始时，在步骤400，移动节点200接收表示移动节点不再连接至LAN206的解除连接通知。该解除连接通知可从多种环境中的任何一种产生，包括，作为示例，用户断开了移动节点200和LAN 206之间的网络连接。作为响应，移动节点200上的网络通信协议栈处理该解除连接通知并发布通知到移动节点200上受影响的组件。作为示例，当接收解除连接通知时，协议栈组件或者驻留在上述协议栈中的应用程序会产生一对话框来邀请用户建立一个新的连接。在一个示例实施例中，对话框展现了一组可用的与用户进行通信的网络/接口/模式。还需要注意，在一些示例中，NDIS和TCP/IP栈可能不会接收解除连接通知（例如，移动无线）。作为取代，移动节点将会从新的接入点接收媒体连接通知。

[0052] 继续本示例，在步骤402用户（或者可能是在移动节点200上执行的标准驱动(criterion-driven)的自动化网络选择组件）选择新的网络，与该网 络将建立连接。在示出的示例中，用户选择和传输塔202相关的蜂窝网络。之后执行一组步骤来建立至节点200的本地网络(LAN 206)的新连接和通过该新的网络连接至相应的节点的连接。

[0053] 在步骤404期间，移动节点200连接/注册至蜂窝无线网络（具有和LAN206不同的安全区域）并被动态地分配不同于其本地网络地址(1111)的在蜂窝网络上的新的网络地址（例如，3331）并进行配置。用于新网络的DNS服务器被更新以包括移动节点在其名称解析表中的新地址（以及在新的安全区域内移动节点的名称）。因此，例如，在移动节点解除通过无线收发机204从LAN 206的连接并通过传输塔202重新连接至该蜂窝网络的情况下，分配给移动节点200的网络地址从本地地址“1111”变成远程网络地址“3331”。

[0054] 此后，在步骤406确定移动节点200目前驻留在移动节点200的本地网络(LAN 206)的安全区域之外。按照本发明的一实施例，移动节点200通过按照有移动节点200维持的策略来检验其新的网络地址和配置以确定它已经移动到了其本地网络的安全区域之外（例如，之前建立连接的对应节点的安全区域）。例如，移动节点200上的策略说明，当当前分配的IP地址表示不同于11xx的网络时，移动节点200需要考虑其自己处于不同的安全区域中。该策略还进一步指定其应该连接的VPN服务器的IP地址为1150。

[0055] 在步骤408，在移动节点200上执行的VPN客户机360初始通过与例如网关/防火墙/调制解调器210相关执行的VPN服务器建立VPN隧道连接。VPN服务器连接在移动节点200向VPN服务器提供一组注册标准(logoncredential)之后被建立。响应于成功的注册，VPN服务器通过动态主机配置协议(DHCP)进程--或者诸如点对点协议(PPP)的多种协议中的任何一种在LAN 206上建立用于节点200的新连接，例如1115。因此，在完成步骤408之后，VPN服务器作为用于LAN 206上的移动节点200的可信的消息发送者。作为移动节点200可信的消息发送者，VPN服务器提供用于LAN 206上的节点200的授权、安全以及消息集成服务。

[0056] 之后，在步骤410期间，移动节点200通过VPN隧道连接将其新的网络地址(1115)提供给其授权DNS服务器209。如上面所描述的，按照本发明的一个实施例，移动节点表示在步骤410期间，非授权DNS服务器不应 该缓存网络节点的新的网络地址(1115)。在本发

明的一具体实施例中，该功能由指定 TTL 为 0 的移动节点 200 实现。结果，试图具有移动节点的地址的节点将仅仅依靠授权的 DNS 服务器 209 来提供移动节点 200 的地址。

[0057] 此后，在步骤 412，如果需要的话，移动节点 200 通过发布捆绑更新至对应节点的最后所知的地址来重新建立至对应的节点的潜在丢失的连接。该捆绑更新通知对应的节点分配给移动节点的新地址 (1115)-- 在完成步骤 408 之后用于移动节点 200 的 VPN 服务器地址。如果对应的节点也改变了其地址（例如，移动节点 214 在与移动节点 200 基本上相同的时间也移动了），则捆绑更新会失败。移动节点 200 发布识别分配给对应节点的唯一名称的名称查询。如果返回的名称查询地址与由移动节点当前维持的对应节点的地址不相同，则移动节点使用所提供的地址来发布另一个捆绑更新。在接收到捆绑更新响应时，移动节点和对应节点之间的连接在步骤 414 期间被保存。

[0058] 需要注意作为潜在的优化（特别是如果移动节点 200 感觉到捆绑更新的目标接收者同样是移动的），不是等待初始的捆绑更新请求失败，移动节点 200 在接收对于初始捆绑更新请求的响应之前执行名称查询。如果对于名称查询的响应不同于在初始的捆绑更新请求期间使用的地址，则移动节点 200 发布进一步的捆绑更新请求。这样的优化，尽管通常会导致不必要的名称请求，但加快重新连接至一对应的节点也被重新定位。该优化可进一步被修整为仅仅基于应用程序的相关容忍度 (tolerance) 而触发，该容忍度是关于在移动节点 200 重新定位时至对应节点的连接瓦解长度。上述的用于重新建立连接的安排和方法，使用在动态网络环境中的 DNS 和 VPN 服务器组件，使得移动节点能在在移动节点移动到位于其本地网络以外的位置时重新建立至对应节点的连接而不依靠本地代理。

[0059] 转到图 5，其是一组示例通信 / 动作，描述用于两个移动节点改变在基本上相同的时间改变它们的位置的情况。初始时，移动节点 A 和 B（例如，移动节点 200 和 214）被配置了它们的主 DNS 后缀。节点 A 和 B 还具有用于它们的每个适配器的连接专用 DNS 后缀。该后缀确定它们的附件 DNS 区域的当前点。节点 A 和 B 注册到它们分别的授权 DNS 服务器 500 和 502（它们可能是相同的服务器）。移动节点指示叶 DNS 服务器通过指定 TTL 为 0 而不缓存它们的地 址。一连接基于它们的当前地址而在节点 A 和 B 之间建立。

[0060] 然而，在步骤 1a、1b，节点 A 和 B 改变了它们的地址。之后，在步骤 2a、2b，节点 A 和 B 获得并注册它们的新地址至它们的授权 DNS 服务器。在步骤 3a、3b 期间，节点 A 和 B 中的每一个相互发布捆绑更新，但是捆绑更新的目的地是每一个节点的旧地址。因此捆绑更新会失败（潜在会有多次）。

[0061] 在步骤 4a、4b 期间，节点 A 和 B 的每一个询问它们的 DNS 服务器 500 和 502 以获得它们所希望的目标的当前地址。因为每一个节点都指定 TTL 为 0，DNS 服务器 500 和 502 在步骤 5a 和 5b 期间传动请求至用于该移动节点的授权 DNS 服务器。在步骤 6a、6b 期间，授权 DNS 服务器 500 和 502 返回节点 A 和 B 的新地址。名称询问响应在步骤 7a、7b 期间被传回节点 A 和 B。

[0062] 现在获得了移动的节点的最新的地址，节点 A 和 B 在步骤 8a、8b 期间重新发布它们的捆绑更新并在步骤 9a、9b 期间接收它们的捆绑更新的成功确认。需要注意仅仅需要节点 A 或者节点 B 的捆绑更新中的一个被发布 / 确认以重新建立（当两个节点移动时）瓦解的连接，由于捆绑更新的接收者将在此更新中获得发送者的新地址。还需要注意，按照之前描述的优化，节点不需要在发布名称询问以获得节点更新的网络地址之前等待一个或者更

多的捆绑更新失败。

[0063] 快速 VPN 隧道再使用

[0064] 对于之前公知支持移动节点的系统的另一个增强涉及对 VPN 隧道的操作。具体地说，按照本发明的一个实施例，移动节点的 VPN 隧道在移动节点从地址一个外部转交 (care of) 地址移动到地址的另一个外部转交 (care of) 地址时会快速的重设置。快速 VPN 重设置功能由位于由移动节点实现的通信栈的 TCP/IP 层 340 的顶部的因特网安全组件（例如，IPSEC）部分地支持。

[0065] 在下列情况下移动节点 200 可自动并快速地建立 VPN 连接：(1) 具有将要与之建立 VPN 隧道的在 LAN 206 上的 VPN 服务器的地址，以及 (2) 在移动节点 200 和 VPN 服务器之间的网络接入服务器（以及任何干涉网络）允许移动节点接入到 VPN 服务器。这样的接入通过提供 VPN 服务器地址作为移动节点 200 的配置的一部分来辅助。该地址可以多种方式中的任何一种被提供，包括通过配置用户接口人工提供、来自 DHCP 服务器、通过策略下载。此外，移 动节点连接的网络提供至因特网的连接。用于移动节点 200 连接至的外部网络的授权服务器被配置为对于通过 VLAN 或者 VPN 的节点支持至因特网的客人连接并因而支持至 LAN 206 的 VPN 服务器的连接。此后，移动节点 200 潜在地使用嵌套的 VPN（例如，在客人连接是通过 VPN 的情况下）连接至 LAN 206 的安全区域中的节点。作为示例，L2TP/IPSEC 或者 IPSEC 隧道模式 VPN 连接被建立。

[0066] 针对 VPN 连接设置的性能优化使得在其网络地址改变时，快速再使用所建立的用于移动节点 200 安全数据结构。这种优化通过下列的对于存在的支持网络通信的协议栈的增强来辅助。首先，位于 TCP/IP 层 340 的顶端的互连网安全组件（例如，IPSEC）在处理移动节点 200 的本地地址之后被调用，而对于移动节点 200 的不会改变的本地地址被用于授权该移动节点用于 VPN 隧道。因特网 SA（安全关联）是用于机器之间的安全会话环境。指定用于 IP 安全 SA 的属性包括，但不限于，IP 地址、授权机制、加密算法、算法模式以及密钥素材。基于本地地址的因特网 SA 在移动节点 200 改变其地址时不会改变。因此不需要在移动节点改变其地址时更新安全结构（例如，IPSEC 过滤器）。

[0067] 第二，之前建立的在移动节点 200 和在 LAN 206 上的 VPN 服务器之间的 VPN 隧道被再使用。在本发明的一个实施例中，移动节点 200 和 LAN 206 上的 VPN 服务器之间的第二层隧道协议 (L2TP) 隧道在移动节点 200 按照移动 IPv6 规则在转交地址之间移动时维持。移动节点 200 使用本地安全区域之外的其节点的第一转交地址作为其本地地址。其指定第一转交地址作为其本地地址并将其用于隧道和安全结构以建立 VPN 隧道。因此 IPSEC 过滤器被使用该本地地址建立。

[0068] 转到图 6，概述了当移动节点多次改变其在公共网络中的地址时，由上述的对 VPN 操作的增强所支持的快速 VPN 隧道再使用方法。初始时，在步骤 600 期间移动节点 200 在第一外部转交地址建立至 LAN 206 上的 VPN 服务器的 VPN 隧道（例如，L2TP 隧道端点）。移动节点使用第一外部转交地址作为其针对外部区域的本地地址。

[0069] 在步骤 602，移动节点 200 改变其地址至第二外部地址。在步骤 604，移动节点 200 发送捆绑更新至其 VPN 服务器 / 隧道端点。捆绑更新按照，例如 Ipv6 映射第一地址至第二地址。响应于捆绑更新，在步骤 606VPN 服务器改变其映射（原始是第一至第一地址）来映射第一地址至新的第二地址，但是维持所有的之前在 VPN 隧道被在第一外部转交地址创建

用于移动节点时创建的原始互连网协议安全结构（例如，源地址 -- 外部网络上第一转交地址 -- 建立 VPN 隧道的客户机和与该客户机在其之前的地址相关的其他区域）。隧道结构同样被再使用。这种隧道结构的示例包括下列类型：隧道 (L2TP、IPSEC)、客户机的 IP 地址、隧道服务器的 IP 地址、（可选择的）在两个端（如果是 L2TP 隧道协议）的端口、所使用的安全的种类（例如 IPSEC)。总之，当移动客户机的地址改变时，本发明维持适当的之前产生的隧道结构。这是通过总是使用本地地址来查找该结构来辅助（例如，在查找之前取代 IP 地址头部中的本地地址）。

[0070] 此后，VPN 服务器将附加一个路由扩展头部，目的头部可选择地指定第一地址作为发送到移动节点 200 的新（第二）地址的所有分组的 IPv6 头部的目的地址。

[0071] 在步骤 608，当在第二地址时移动节点 200 接收这样的分组时，IP 层使用第一（外部本地）地址来替换第二地址用于该移动节点。修改后的节点之后传送给 IP 层（例如，TCP、UDP 等等）的客户机。因此，当移动节点 200 确实不再处于第一外部转交地址时，IP 层的客户机继续相信移动节点 200 仍然处于其第一地址。

[0072] 在步骤 610，当移动节点 200 发送分组至 VPN 服务器用于 LAN 206 时，移动节点 200 将第一地址放置到附加到 IPv6 头部的主机扩展头部的“本地地址”选项中。第二，移动节点的新地址被放置于所传送的分组中的 IPv6 头部的源地址中。

[0073] 在步骤 612，当 VPN 服务器接收所传送的分组时，IPv6 栈组件在将所接收的分组传送到通信栈的更加高的层之前使用第一地址来替换在源字段中的第二地址。再一次，更高的层的栈的组件（负责进行用隧道传输、认证对于通过该隧道传输的分组的授权并过滤未授权的分组），诸如 L2TP 和 IP 安全过滤，不会感知到移动节点 200 的地址的变化。因此，原始创建的用于移动节点 200 和用于 LAN 206 的 VPN 服务器之间的 VPN 隧道的隧道和安全结构继续工作。

[0074] 参考许多可能的计算环境，其中本发明的原理可被应用且灵活地实现网络接入配置的以满足在一包括多个移动节点的网络环境中维持地址和连接的挑战，需要认识到此处描述的实施例意味着是说明性的并不应该被作为对于本发明的范围的限制。熟悉应用本发明的领域的技术人员将会理解示出的实施例可在顺序上修改或者在细节上修改而不脱离本发明的原理。因此，此处描述的本发明预见了所有的这种实施例，其可以在权利要求或其等价描述的范围之内。

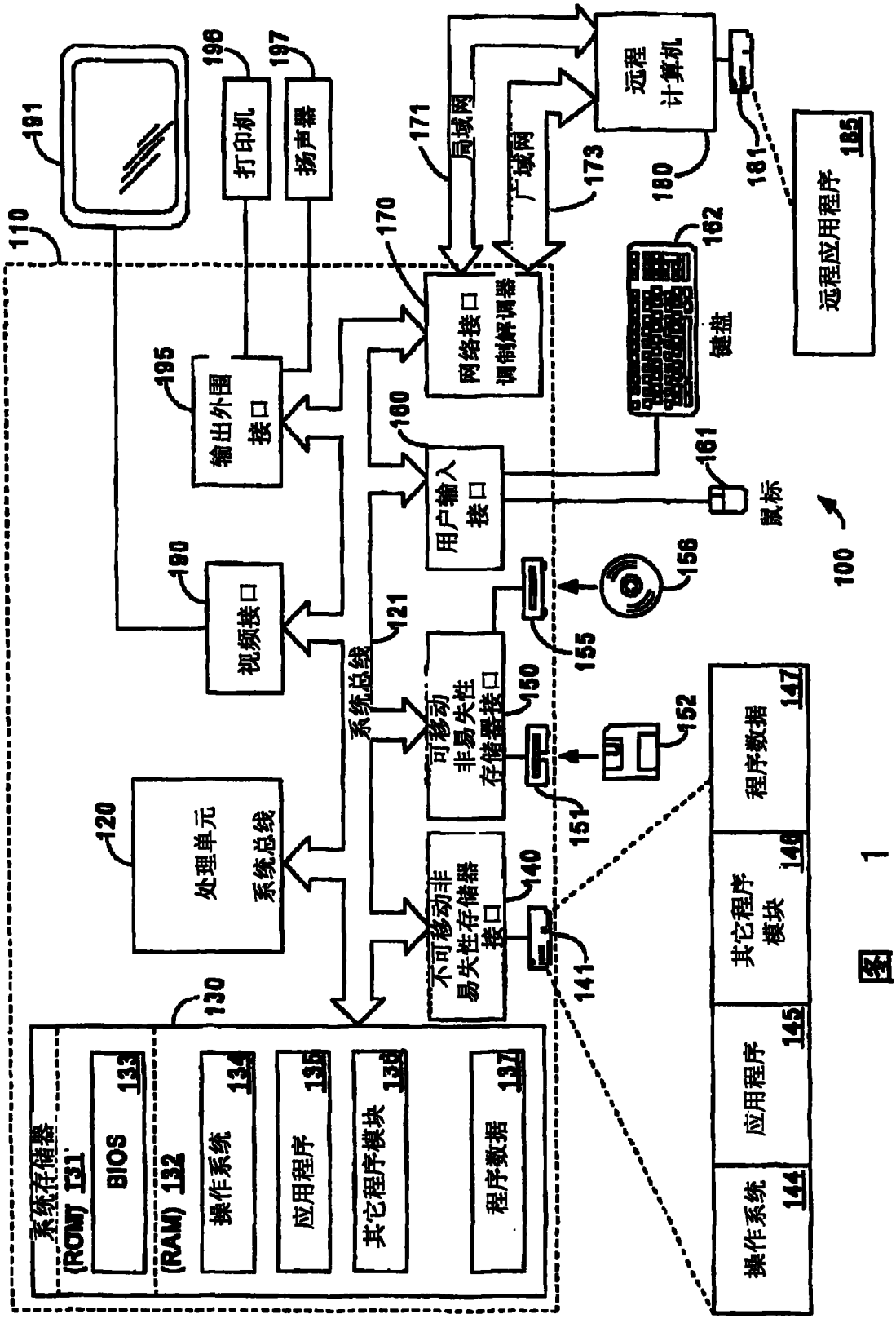

110
191
196
打印机
197
扬声器
171
局域网
远程计算机
173
广域网
180
181
远程应用程序
185
162
键盘
170
网络接口
调制解调器
195
输出外围接口
160
用户输入接口
161
鼠标
100
190
视频接口
121
系统总线
156
155
可移动非易失性存储器接口
150
152
151
120
处理单元
系统总线
不可移动非易失性存储器接口
140
141
130
系统存储器
(ROM) 131
BIOS 133
(RAM) 132
操作系统 134
应用程序 135
其它程序模块 136
程序数据 137
程序数据 147
其它程序模块 146
应用程序 145
操作系统 144

图 1

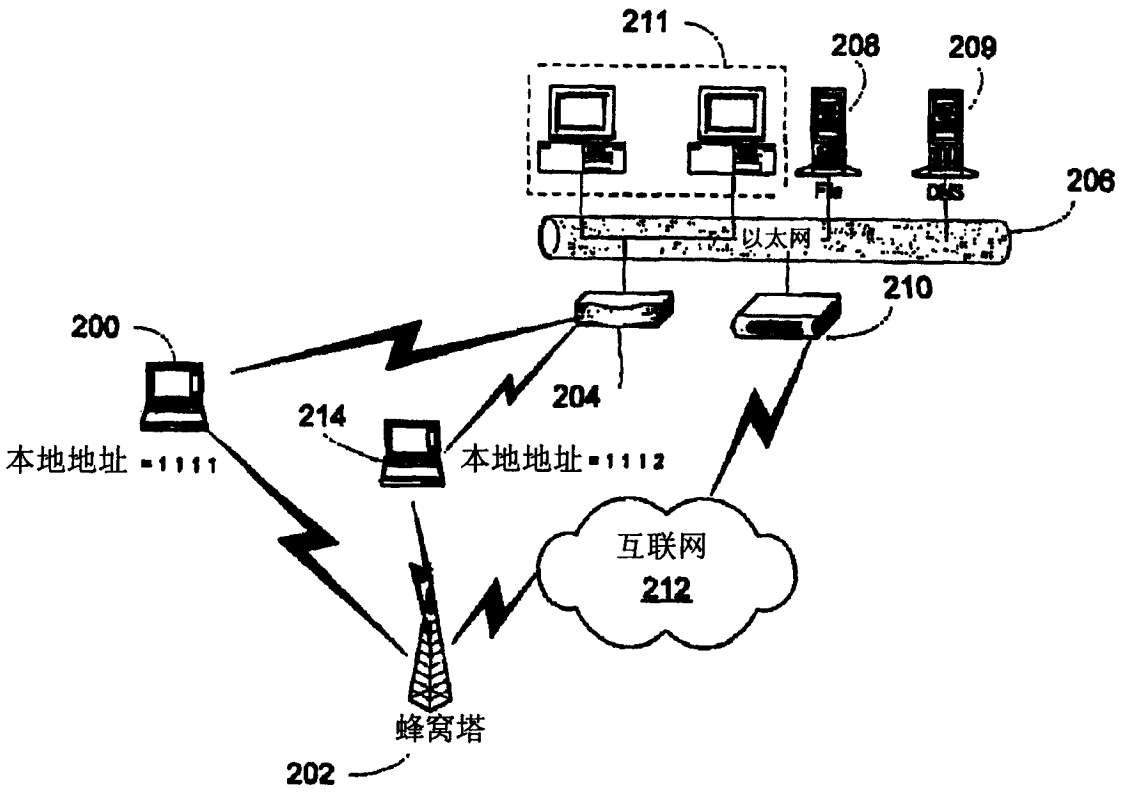

211
208
209
206
File
DNS
以太网
210
200
204
214
本地地址 =1111
本地地址 =1112
互联网
212
蜂窝塔
202

图 2

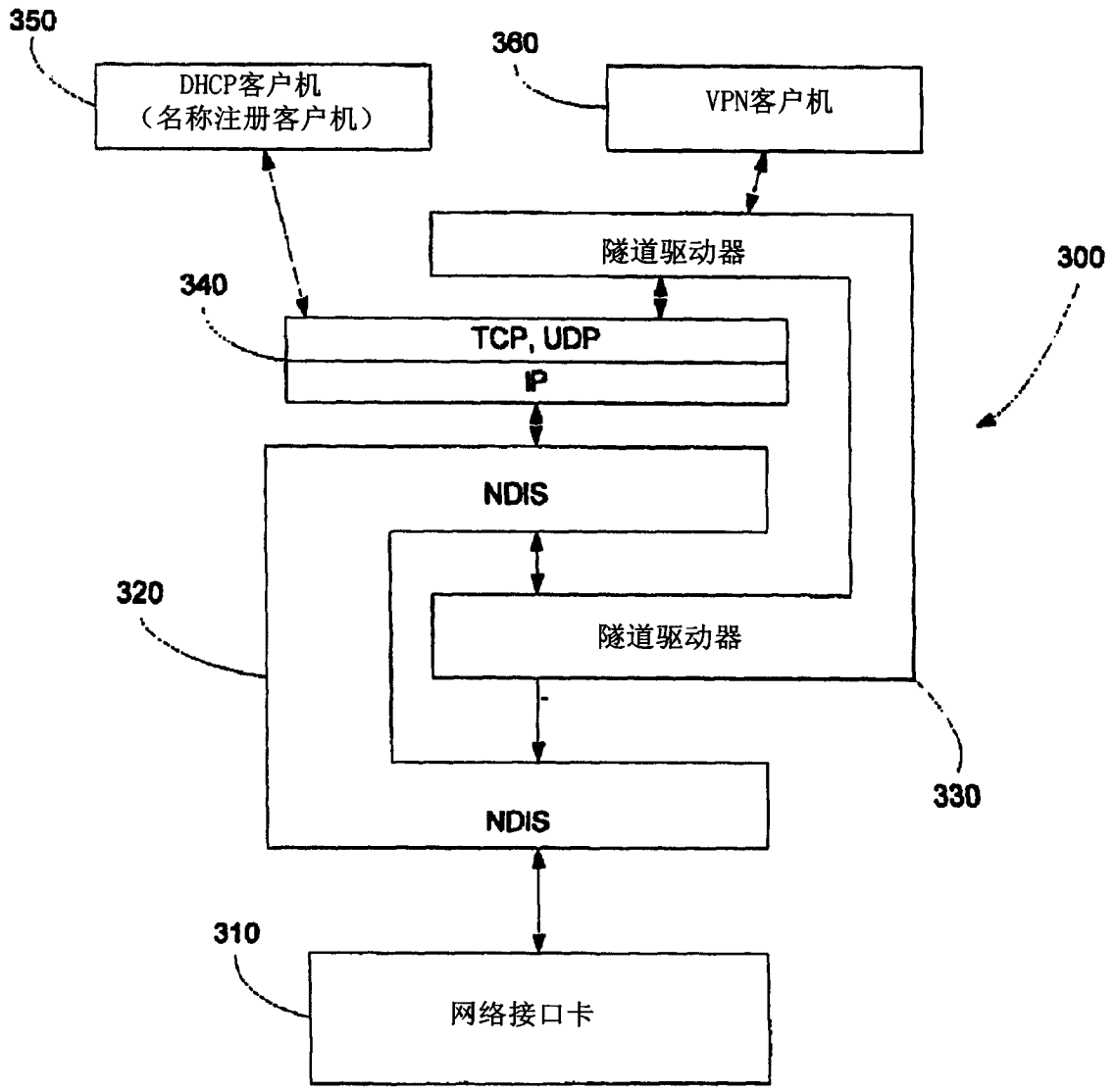

350
DHCP客户机
（名称注册客户机）
360
VPN客户机
隧道驱动器
300
340
TCP, UDP
IP
NDIS
320
隧道驱动器
330
NDIS
310
网络接口卡

图 3

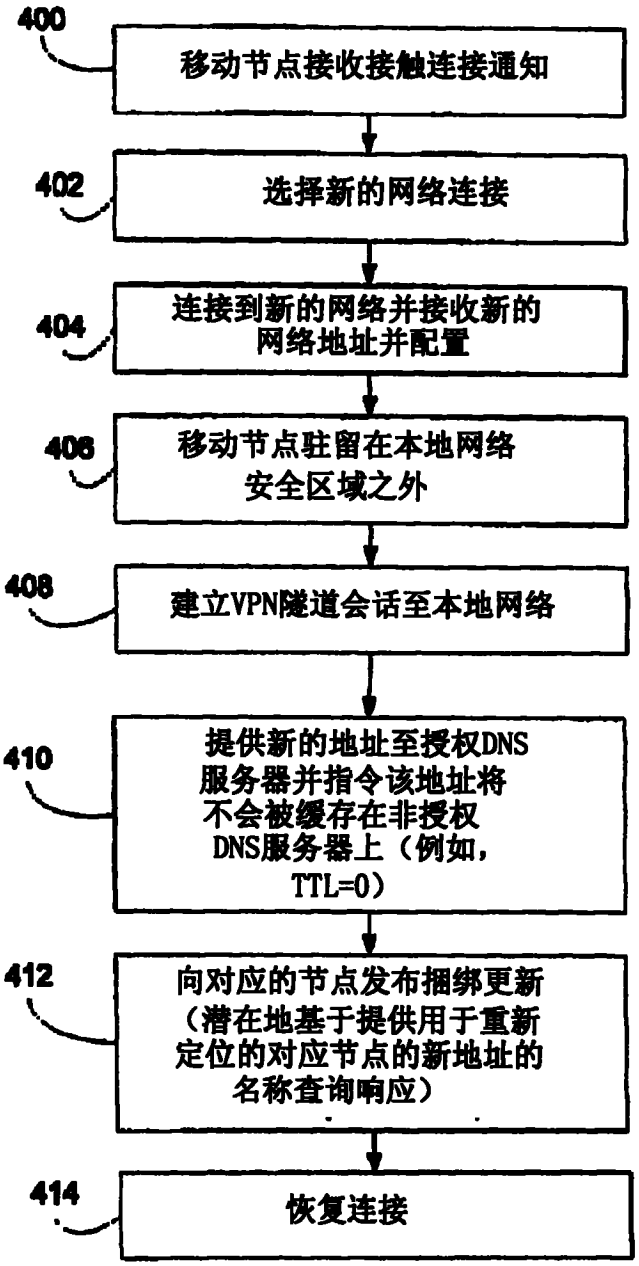

400
移动节点接收接触连接通知
402
选择新的网络连接
404
连接到新的网络并接收新的网络地址并配置
406
移动节点驻留在本地网络安全区域之外
408
建立VPN隧道会话至本地网络
410
提供新的地址至授权DNS服务器并指令该地址将不会被缓存在非授权DNS服务器上（例如，TTL=0）
412
向对应的节点发布捆绑更新（潜在地基于提供用于重新定位的对应节点的新地址的名称查询响应）
414
恢复连接

图 4

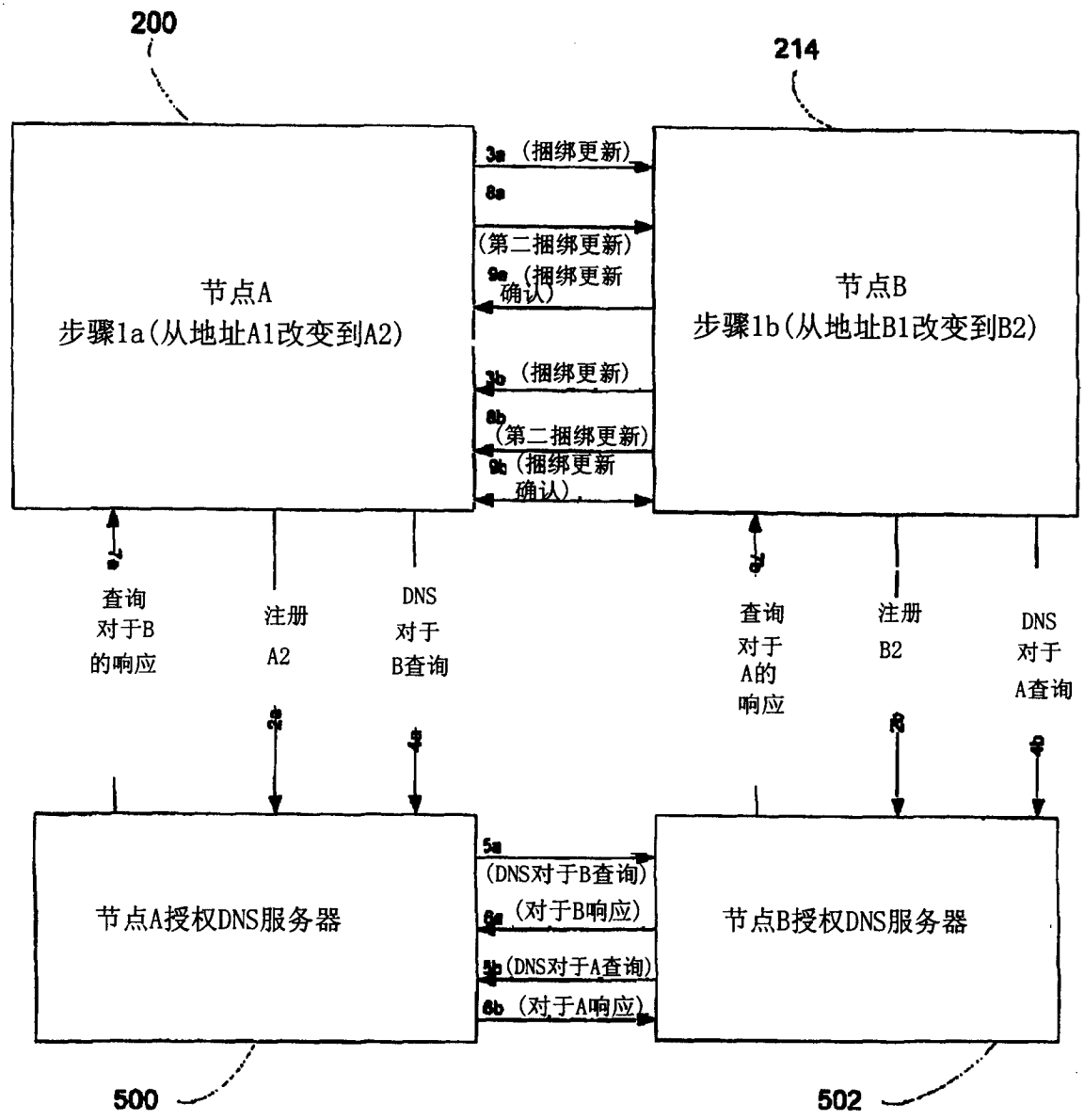

200
214
节点A
步骤1a(从地址A1改变到A2)
节点B
步骤1b(从地址B1改变到B2)
3a (捆绑更新)
8a
(第二捆绑更新)
9a (捆绑更新确认)
3b (捆绑更新)
8b (第二捆绑更新)
9b (捆绑更新确认)
查询对于B的响应
注册A2
DNS对于B查询
查询对于A的响应
注册B2
DNS对于A查询
5a (DNS对于B查询)
6a (对于B响应)
5b (DNS对于A查询)
6b (对于A响应)
节点A授权DNS服务器
节点B授权DNS服务器
500
502

图 5

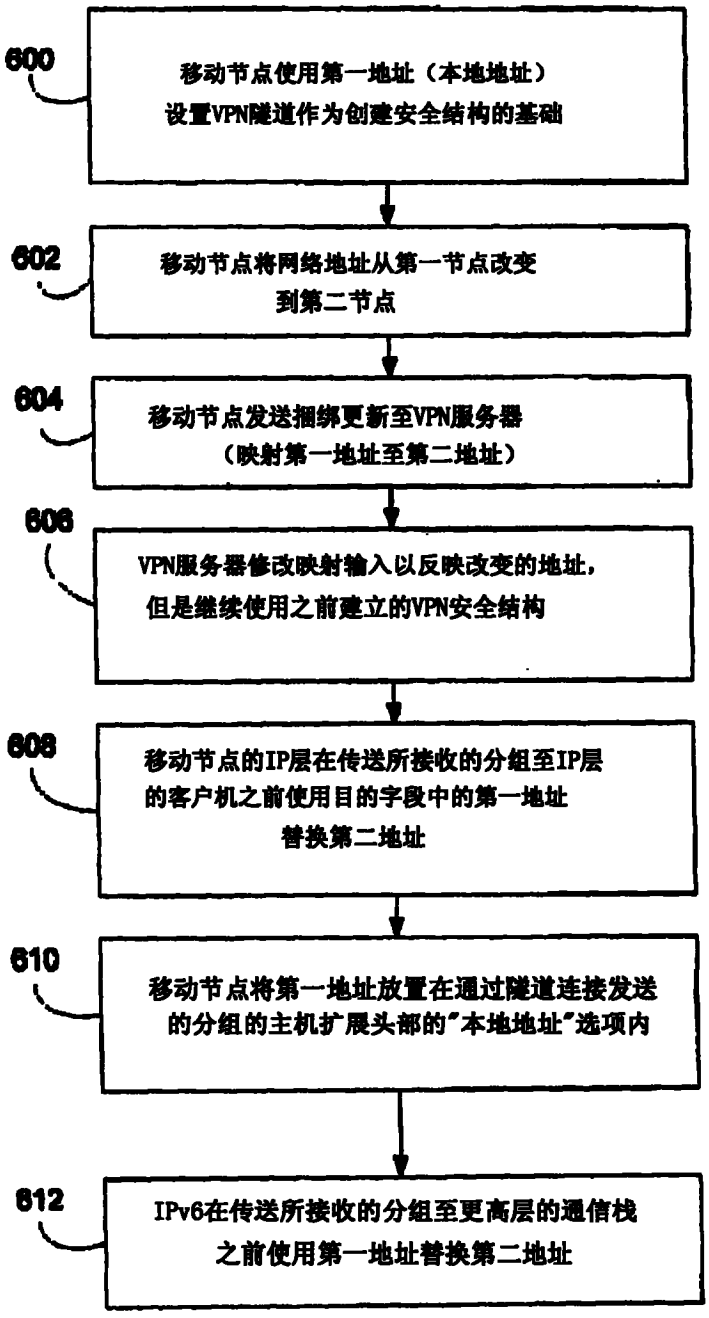

600
移动节点使用第一地址（本地地址）
设置VPN隧道作为创建安全结构的基础
602
移动节点将网络地址从第一节点改变
到第二节点
604
移动节点发送捆绑更新至VPN服务器
（映射第一地址至第二地址）
606
VPN服务器修改映射输入以反映改变的地址，
但是继续使用之前建立的VPN安全结构
608
移动节点的IP层在传送所接收的分组至IP层
的客户机之前使用目的字段中的第一地址
替换第二地址
610
移动节点将第一地址放置在通过隧道连接发送
的分组的主机扩展头部的"本地地址"选项内
612
IPv6在传送所接收的分组至更高层的通信栈
之前使用第一地址替换第二地址

图 6