[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 13/14

[12] 发明专利申请公开说明书

[21] 申请号 01819703.5

[43] 公开日 2004 年 2 月 25 日

[11] 公开号 CN 1478232A

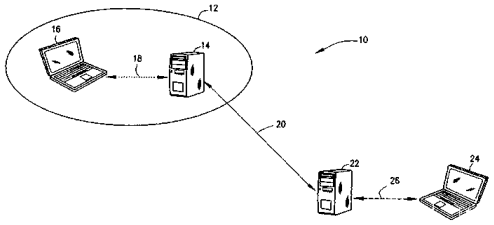
[22] 申请日 2001.11.13 [21] 申请号 01819703.5
[30] 优先权
[32] 2000.11.13 [33] US [31] 60/247,008
[86] 国际申请 PCT/US01/43066 2001.11.13
[87] 国际公布 WO02/42861 英 2002.5.30
[85] 进入国家阶段日期 2003.5.28
[71] 申请人 ECUTEL 公司
地址 美国弗吉尼亚州
[72] 发明人 高里·马基安尼 拉维·纳加拉健
张 强 哈里·加蒂 德尊·塔兰
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 蒋世迅

权利要求书 4 页 说明书 9 页 附图 7 页

[54] 发明名称 用于安全网络移动性的系统和方法

[57] 摘要

当移动客户漫游至原籍网络以外，到达新位置时，本发明提供一种在原籍网络与移动客户之间，保持安全通信的系统和方法。本发明的一种方法，包括的步骤有：为新的客户位置建立新的 IP 地址，发送标识该新 IP 地址位置的注册消息；鉴证该注册消息；把该注册消息封装，并发送至原籍服务器；把新 IP 地址作为转交地址，为客户在原籍服务器上注册；确认伴随该客户的新 IP 地址的注册；在原籍服务器与中继服务器之间，代表该客户建立安全关联；在客户的永久 IP 地址与客户的新 IP 地址之间，执行网络地址转换；根据为该客户建立的安全关联及地址转换，把访问该客户的分组，在原籍服务器及中继服务器之间隧穿；最后，在中继服务器上把分组解封装，并把分组转发至该客户。



ISSN1008-4274

1. 在一种计算机网络布局中包括：至少有一个原籍网络服务器的原籍网络及保护所述原籍网络服务器的防火墙、在所述原籍网络以外的中继服务器、和在所述原籍网络内有永久IP地址的客户，在该种计算机网络布局中，当所述客户在所述原籍网络之外漫游，到达新的位置时，一种在该原籍网络服务器与该客户间保持安全通信的方法，所述方法包括:

为新的客户位置建立新的IP地址;

向所述中继服务器发送注册消息，标识所述新IP地址位置;

鉴证所述注册消息;

封装并发送所述注册消息至所述原籍服务器;

把所述新IP地址作为转交地址，为所述客户在所述原籍服务器注册;

确认伴随所述客户的所述新IP地址的注册;

在所述原籍服务器与所述中继服务器之间，代表所述客户建立安全关联;

在客户的永久IP地址与客户的新IP地址之间，执行网络地址转换;

根据已为所述客户建立的安全关联和所述地址转换，把访问所述客户的分组，在所述原籍服务器与所述中继服务器之间隧穿；和

把所述分组在所述中继服务器上解封装，并把所述分组转发至所述客户。

2. 按照权利要求1的方法，其中所述原籍网络还包括复用器子系统。

3. 按照权利要求1的方法，其中，从所述客户到所述原籍服务器的通信的至少一部分，是按HTTP请求格式。

4. 按照权利要求3的方法，其中，从所述原籍服务器到所述客户的通信的至少一部分，是按HTTP响应格式。

5. 按照权利要求 4 的方法，其中，从所述客户到所述原籍服务器的通信的至少一部分，是封装在 UDP 分组中。

6. 按照权利要求 5 的方法，其中，从所述原籍服务器到所述客户的通信的至少一部分，是封装在 UDP 分组中。

7. 按照权利要求 1 的方法，其中所述方法还包括步骤：设置网络网关，其中所述网络网关的操作，是把分组隧穿所述防火墙，到达所述原籍服务器。

8. 按照权利要求 7 的方法，其中所述网络网关是 Virtual Private Network 网关。

9. 在一种计算机网络布局中包括：至少有一个原籍网络服务器的原籍网络及保护所述原籍网络服务器的防火墙、在所述原籍网络以外的中继服务器、和在所述原籍网络内有永久 IP 地址的客户，在该种计算机网络布局中，当所述客户在所述原籍网络之外漫游，到达新的位置时，一种在该原籍网络服务器与该客户间保持安全通信的方法，所述方法包括：

为新的客户位置建立新的 IP 地址；

向所述原籍服务器发送注册消息，标识所述新 IP 地址位置；

封装并发送所述注册消息至所述原籍服务器；

把所述新 IP 地址作为转交地址，为所述客户在所述原籍服务器注册；

确认伴随所述客户的所述新 IP 地址的注册；

在所述原籍服务器与所述客户之间建立安全关联；

在客户的永久 IP 地址与客户的新 IP 地址之间，执行网络地址转换；和

根据已为所述客户建立的安全关联和所述地址转换，把访问所述客户的分组，在所述原籍服务器与所述客户之间隧穿。

10. 按照权利要求 9 的方法，其中所述原籍网络还包括复用器子系统。

11. 按照权利要求 9 的方法，其中，从所述客户到所述原籍服务

器的通信的至少一部分，是按 HTTP 请求格式。

12. 按照权利要求 11 的方法，其中，从所述原籍服务器到所述客户的通信的至少一部分，是按 HTTP 响应格式。

13. 按照权利要求 12 的方法，其中，从所述客户到所述原籍服务器的通信的至少一部分，是由所述复用器子系统封装在 UDP 分组中。

14. 按照权利要求 13 的方法，其中，从所述原籍服务器到所述客户的通信的至少一部分，是由所述复用器子系统封装在 UDP 分组中。

15. 按照权利要求 9 的方法，其中所述方法还包括步骤：设置网络网关，其中所述网络网关的操作，是把分组隧穿所述防火墙，到达所述原籍服务器。

16. 按照权利要求 15 的方法，其中所述网络网关是 Virtual Private Network 网关。

17. 一种为客户保持安全通信的系统，该客户在原籍网络系统内有一永久 IP 地址，又当该客户在所述原籍网络系统之外漫游时，有一临时的、转交的 IP 地址，所述系统包括：

原籍网络服务器，其中，所述原籍网络服务器鉴证漫游至所述原籍网络系统外的客户发来的消息，同时在客户的永久 IP 地址与客户注册的转交 IP 地址之间，执行网络地址转换，还有，其中所述原籍网络服务器，把访问所述客户永久 IP 地址的消息，封装并再发送至客户注册的转交 IP 地址；

中继服务器，所述中继服务器位于所述原籍网络之外，其中，所述中继服务器在所述原籍网络服务器与所述客户之间隧穿消息；和

复用器子系统，其中，所述复用器子系统由 HTTP 服务器和复用器模块构成。

18. 一种在漫游的客户与原籍服务器之间通信的方法，其中，客户或原籍服务器中至少一个受防火墙保护，所述方法包括：

按 HTTP 请求格式产生第一消息；

通过所述防火墙发送所述 HTTP 请求格式的消息；

处理所述第一消息，其中，所述第一消息被封装在 UDP 分组中

并转发至它的指定接收者;

响应所述第一消息，产生第二消息，其中所述第二消息被封装在UDP分组中;

把所述第二消息转换为HTTP响应格式;

把所述第二消息发送至它的指定接收者。

19. 按照权利要求1的方法，其中，所述方法还包括步骤:

按HTTP请求格式产生第一消息;

通过所述防火墙发送所述HTTP请求格式的消息;

处理所述第一消息，其中，所述第一消息被封装在UDP分组中并转发至它的指定接收者;

响应所述第一消息，产生第二消息，其中所述第二消息被封装在UDP分组中;

把所述第二消息转换为HTTP响应格式; 和

把所述第二消息发送至它的指定接收者。

20. 按照权利要求9的方法，其中，所述方法还包括步骤:

按HTTP请求格式产生第一消息;

通过所述防火墙发送所述HTTP请求格式的消息;

处理所述第一消息，其中，所述第一消息被封装在UDP分组中并转发至它的指定接收者;

响应所述第一消息，产生第二消息，其中所述第二消息被封装在UDP分组中;

把所述第二消息转换为HTTP响应格式; 和

把所述第二消息发送至它的指定接收者。

用于安全网络移动性的系统和方法

技术领域

本发明一般涉及增强计算机网络移动性的系统和方法。更具体说，本发明涉及提供安全的、互连网协议（IP）移动性的系统和方法。

背景技术

用于移动 IP 的目前标准，能使移动用户通过互连网漫游时保持连接，还能以同一 IP 地址连接至移动用户。因此，移动 IP 的目前系统有利于双向通信，也支持移动服务器（或路由器或其他网络资源）。

移动 IP（Mobile IP）是开放的互连网标准，主要内容在 ITEF-RFC 2002 中规定，本文引用该标准，供参考。移动 IP 的基本前题是，不论移动用户漫游到何处，他能够保持同一网络地址。基于两个原因，这一能力是十分重要也是十分必要的：（1）当从一个网络漫游至另一个网络时，能够保持连接，和（2）能够双向通信。例如用户数据报协议（UDP）和传输控制协议（TCP）等基于 IP 的通信协议，连接能够保持。对这些协议，连接是通过四个参数标识的，即源与目的地 IP 地址，及源与目的地端口号码。没有移动 IP，在漫游时，要求改变移动用户的 IP 地址，随之导致丢失先前 IP 地址建立的连接。因此，移动 IP 保持同一 IP 地址的能力，在保持漫游时的连接的意义下，能提供“无缝隙”网的漫游。保持单一 IP 地址的另一个好处，是真正的双向通信。这一点意味着，能够把漫游的移动装置（本文此后称为“客户”）作为目的地而建立连接。该种能力是交互式应用程序（类似 MS NetMeeting、CUSeeMe、PowWow、及其他）的关键。该种能力同样为各种移动信息服务器铺平道路。实现所有基于 IP 的应用程序都具有这些好处，是十分重要的。从应用程序，因而也从用户的角度看，前景是，只需用标识每一客户（即，便携电脑、移动电话手持机、智能电话）的单一的、永久的 IP 地址，无需理会客户的位置。

移动 IP 通过采用两个 IP 地址而工作：一个永久 IP 地址，对于应用程序和用户是可见的，而第二个临时的或转交的地址，则用于确保适当的路由。因此，当一方离开它们的原籍网络漫游，它们的客户建立一新的 IP 地址，且该新的 IP 地址作为转发地址，把访问原先的、永久的 IP 地址的所有消息业务量，转发回它们的原籍网络。因此，移动用户将获得路由至它们的分组，仿佛它们仍旧与它们的原籍网络终端连接一样。操作时，移动 IP 软件在两个地址之间判断，并隐藏移动性，使应用程序与用户不能察觉。

在大多数应用程序中，移动 IP 通过驻留在移动用户原籍网络中的软件工作。该种软件（有时称之为“代理”）为已离开的客户截接到达的分组，并把它们转发至它们的转交地址。在某些情况中，移动 IP 包括使用驻留在漫游客户访问的各个子网上的移动 IP 软件（称为“外部代理”）。在许多情况下，外部代理的使用不是严格必需的，因为它的功能可以包括在客户自身中。没有外部代理的客户的操作，被称为处于局内模式。

移动 IP 协议的力量显然在于它能进行无缝隙漫游和双向通信。但是，从实际的远景看，单靠移动 IP 本身是不适当的。最重要的是，移动 IP 已经设计供开放的互连网使用。在它的说明书中，很少考虑安全性。实际上，移动用户的通信必须受到保护，避免窃听和窜改。

正如目前的配置和实践，除了没有为它自身网络提供安全性外，移动 IP 网络不提供任何实际装置，用于安全地接入与它通信的受保护的公司联合网。具体说，移动 IP 协议是不能通过诸如防火墙或 VPN 网关等装置工作的，而这些装置越来越普遍。

发明内容

按照本发明，提供一种系统和方法，用于安全的 IP 移动性，能使漫游用户安全地接入它们的原籍网络。

本发明的另外的优点，是提供一种用于先进的 IP 移动性的系统，它从任何位置和在任何时间，都能提供安全的互连网通信。

本发明的另一个优点，是提供一种用于先进的 IP 移动性的系统，

它提供双向通信。

本发明还有另一个优点，是提供一种用于先进的 IP 移动性的系统，它不会让网络接口的管理来麻烦用户。

本发明的另外的目的和优点，部分将在下面的说明中阐述，部分将从该说明中明显看出，或可由本发明的实践知道。本发明另外的目的和优点，可以通过各种手段和组合，特别是后面权利要求书中指出的各种手段和组合而实现和取得。

附图说明

本发明在某些部件和部件的安排中，将以物理形式表示，它的一个优选实施例将在本说明书中详细说明，并画在构成本说明书一部分的附图中，附图有:

图 1 是简化的示意表示，画出本发明一个实施例使用的计算机网络配置的一个例子;

图 2 是简化的示意表示，画出本发明第二个实施例的计算机网络配置的另一个例子;

图 3 按照本发明的一个实施例，画出一种方法的简化流程图，用于提供安全的网络通信;

图 4 画出一种简化的网络布局，表明用鉴证了的 HTTP 隧道，安全横越防火墙;

图 5 按照本发明的一个优选实施例，画出防火墙安全横越的方法的流程图;

图 6 画出一种简化的网络布局，表明用中继或代理服务器，安全横越防火墙与 VPN 网关;

图 7 画出一种简化的网络布局，表明用 IPSec 网关，安全横越防火墙。

具体实施方式

现在详细参照本发明的本优选实施例，该例子画在附图中，图上相同的参考字符指相同的单元。下面说明的本发明的系统和方法，最好用交互式计算机软件应用程序实施，该交互式计算机软件应用程序，

可以存入如硬盘驱动器、光学媒体如光盘，诸如此类的计算机可读媒体中。还有，该计算机可读媒体可供用户使用，或者在用户的计算机本机上，或者在诸如局域网（LAN）或通过互连网的远程计算机网络上。

本发明的设计，是向移动通信专业人员提供非并行组网支持和安全性的。这一点要求移动性对本发明的用户成为透明的。因此，当本发明的用户离开他的办公室漫游，并到达设有网络的地方时，他能够继续通信而不被中断，也无需重新配置他已启动的装置或客户（即，便携电脑、移动电话手持机、智能电话）。本发明提供一种综合解决方案，一旦移动用户离开他们的公司联合网的保护，便用密码保护他们交换的信息。此外，本发明还提供多种获得接入受保护的公司联合网上资源的手段。

本发明提供一种唯一的且重要的特性，是保持同一网络（IP）地址的能力，如同在公司联合网一样。这一点使本发明成为允许用户接收连接的唯一方案。当移动用户是“呼叫”的接收者时，这一能力在交互式、对等应用程序（类似 MS NetMeeting）中是关键。

图 1 画出一个网络布局 10 的例子，它按照本发明的一个优选实施例，采用本发明的系统和方法。应当指出，本发明的操作与网络部件的任何特定布局或其混合无关，而且为了解释的目的，画在图 1 的该网络 10，纯粹是示例性的并简化了的。

如图 1 所示，示例性网络布局 10 包括原籍网络 12，它又包括原籍网络服务器 14 和位于原籍网络 12 之内的客户 16。如图 1 所示，当在客户 16 的原籍网络 12 中操作时，客户 16 可以经过 LAN 或类似的连接 18，直接与原籍服务器 14 连接。如图 1 进一步所表明，当客户 24 在它的原籍网络 12 之外漫游时，客户 24 仍旧可以经过加密链路 26，中继服务器 22 和加密隧道 20，接入它的原籍服务器 14，下面将参照图 3 详细说明。

图 3 画出的方框图 100，表明本发明的工作原理。在步骤 100，漫游客户 24 为它在它的原籍网络 12 之外的新位置，建立一新的 IP 地

址。在步骤102，客户24向中继服务器102发送标识和注册它的新地址的消息，该中继服务器可以包含与原籍服务器14通信的外部代理。在步骤103，中继服务器22鉴证客户24的消息，以确保客户24的标识。在步骤104，中继服务器22封装客户24的注册消息，并把该封装消息发送至原籍服务器14。在步骤105，原籍服务器14把新IP地址作为客户24的转交地址注册。在步骤106，原籍服务器14向客户发送回答消息，确认所述新IP地址的注册。在步骤107，如下面详细说明的，原籍服务器14和中继服务器22代表所述客户建立安全性关联。在步骤108，原籍服务器14开始在客户24的永久IP地址与客户24的新IP地址之间，对访问客户24的业务量，执行网络地址转换。在步骤109，原籍服务器14和中继服务器22，建立加密隧道20并根据已为客户 24 建立的安全性关联及地址转换，开始对从原籍服务器14到中继服务器22访问客户24的分组，进行封装和隧穿（tunneling）。在步骤110，中继服务器22把隧穿的分组解封装，并经过链路26，把解封装的分组转发至客户，链路26可以是加密的。

参考图2，当中继服务器22由于安全性原因不可用或认为不可靠时，客户24可以按局内模式工作。在该模式中，中继服务器22执行的所有功能，由客户24自身执行。因此，在图2所示的局内模式中，客户24可以直接与它的原籍服务器14通信，注册它的新IP地址（步骤102和103），封装并发送它的注册（步骤104、105、和106），建立与它的原籍服务器14的安全性关联和加密隧道20（步骤107和109），以及把接收的分组解封装（步骤110）。按照本发明，当工作在局内模式时，客户24本身必须获取一拓扑改正的、临时的网络地址。按照本发明的一个优选实施例，客户24可以使用多种手段获得这种地址。例如，客户24可以使用PPP（用于拨号连接），DHCP（用于没有外部代理的 LAN），甚至手动配置一有效的转交地址。在客户 24 获得转交地址之后，本发明的操作便准确地如前所述。

按照本发明的一个优选实施例，在客户24、原籍服务器14与中继服务器22之间发送的所有数据，最好用IPSec ESP协议加密和鉴证。

但是，另外可以用各种加密方法和算法，例如包括，PKI、RSA、DSA、DES、3DES、和 IKE 协议。

此外，按照本发明的一个优选实施例，安全连接即所谓安全性关联的建立，最好按照 Internet Key Exchange（IKE，互连网密钥交换）协议执行。此外，本发明在安全性关联协商时，支持分享机密和数字认证（经 PKI 分配）。最好由本发明的原籍服务器 14 执行 PKI 配置（如加密算法的选择）及管理（如，分享机密或认证管理的分配）。

在建立安全性关联中，IKE 要求两个不同的阶段。第一阶段服务于两个目的。第一，各协商方彼此鉴证，然后，第二，他们协商一中间安全性关联，用于保护第二阶段。按照本发明的一个优选实施例，在 IKE 协商时，最好使用 Public Key Infrastructure（PKI，公共密钥基础结构）数字认证。

当客户 24 漫游进入受防火墙和/或 IPSec（VPN）网关（总的称为“周边防护系统”）保护的网络中时，本发明的补充方面，要求在客户 24 与它的原籍网络服务器 14 之间自由交换分组。按照本发明的一个优选实施例，为安全横越网络周边防护系统提供三种不同方法。简单地说，这些方法是：（a）在鉴证了的 HTTP 隧道中业务量的封装，（b）经过位于鉴证了的防火墙公共侧的代理原籍代理或代理服务器，横越该防火墙，和（c）安全地、基于 IPSec 地横越 VPN 网关。现在参考图 4－7 对每一方法的讨论。

图 4 画出计算机网络布局 10 的方框图，该网络布局按照本发明，使用安全横越网络周边防护的第一种方法。图 5 画出流程图 200，表明本发明的工作原理。在步骤 201，漫游的客户 24 按 HTTP 请求格式产生消息。为本发明的目的，各 HTTPS 响应及请求格式中，考虑一种，也只一种 HTTP 响应及请求格式。

按照本发明的一个优选实施例，该 HTTP 请求格式的消息，最好加密、分组、并封装，以便隧穿。在步骤 202，客户 24 把该 HTTP 请求格式的消息，经 HTTP 链路 51，通过任何介入的防火墙 54、26，发送至它的原籍服务器 14。

按照本发明，因为来自客户 24 的该 HTTP 请求格式的业务量，对防火墙来说仿佛是公共互连网业务量，所以它能成功横越该第一防火墙 54，并最终到达原籍网络的防火墙 26。按照本发明的一个优选实施例，来自客户 24 的 HTTP 请求格式的业务量，首先被原籍网络防火墙 26 用诸如 SOCKS 协议之类鉴证协议，进行鉴证。另外，也可以配置防火墙 26，使它能让 HTTP 请求格式的业务量以或少或多的鉴证度通过。

在步骤 203，一旦通过网络防火墙 26 转发了 HTTP 请求格式的消息业务量，该消息业务量被复用器子系统 44 处理，其中，该消息业务量被封装成 UDP 分组，以便通过 UDP 链路 45 转发至原籍服务器 14。如在图 4 中所示，按照本发明的一个优选实施例，本发明的复用器子系统 44，可以包括 HTTP 客户服务器 50 和复用器 46。此外，复用器子系统 44 如果需要增加网络效率和速度，还可以包括 Fast CGI 模块 48 或其他部件。

在复用器子系统 44 内，如在图 4 中所示，HTTP 服务器 50 最好从原籍网络防火墙 26，经过 HTTP 链路 51，接收该消息业务量。接收后，HTTP 服务器 50 接着路由该消息业务量，以便进一步处理和路由。按照本发明的一个优选实施例，HTTP 服务器 50 最好把该消息业务量路由至 Fast CGI 模块 48，然后，Fast CGI 模块 48 经 TCP 链路 47，把该消息业务量转发至复用器 46。从复用器 46 来的消息，被句法分析成 UDP 分组，并经 UDP 链路 45，转发至原籍服务器 14。

在步骤 204，原籍服务器 14 可以通过产生封装在 UDP 分组中的回答，作为对客户 24 的响应。在步骤 205，该封装的响应被转换为 HTTP 响应格式。如图 4 中所示，该封装的响应，可以如上所述，经复用器子系统 44 转换为 HTTP 响应格式。在步骤 206 中，该封装的响应，接着作为 HTTP 响应格式消息业务量，被转发至它指定的接收者。按照本发明的一个优选实施例，每一 HTTP 链路 51，可以包括强鉴证，以创建安全的 HTTP 隧道。最好在每一防火墙内，提供 SOCKS 协议鉴证或类似的鉴证，并在选择的网和 HTTP 服务器内，使用 Secure

Socket Layer（SSL，安全套接字层）或类似的鉴证。

现在参考图 6，图上画出用作本发明一部分的另外一种防火墙横越方法。如图 6 所示，按照本发明的一个优选实施例，来自客户 24 的 HTTP 请求格式业务量（按“局内”模式画出）可以经过代理或“中继”服务器 32，转发至原籍服务器 14。按照本发明，中继服务器 32 可以按原籍网络 12 如上述相同方式，对客户 24 发送的注册消息进行鉴证。因此，中继服务器 32 可以从客户 24 接收注册消息，并且，如果鉴证成功，中继服务器 32 可以经链路 30，通过防火墙 26，把消息封装并转发至原籍网络服务器 14。之后，按照本发明，原籍网络服务器 14 可以处理该注册消息，并把响应公式化，然后把公式化的响应封装并发送至中继服务器 32。因此，如果该响应指示成功注册，中继服务器 26 的服务器，可以开始在客户 24 与原籍服务器 24 之间，经过加密链路 30 和 34，对隧穿的分组进行中继。按照本发明的一个优选实施例，中继服务器 32 本身，对访问客户 24 和来自客户 24 的分组，执行网络地址转换。再按照本发明的一个优选实施例，紧接注册之后，客户 24 可以开始 IKE 协商，以建立与原籍网络 32 的安全性关联。

至于在代理服务器 32 与原籍服务器 14 之间发送的分组，按照本发明的一个优选实施例，这些分组最好用标准协议类型 4 的封装法（IP-in-IP 封装法）封装。按照本发明，该封装法使用两个 IP 地址、协议号码、和可能甚至硬件地址，可供防火墙非常密实的过滤使用。结果是，即使中继服务器永远受到危害，防火墙整体却不受危害。在另外的实施例中，中继服务器 32 可以纳入防火墙自身之内。

现在参考图 7，图上画出本发明提供的又一个另外的实施例。如在图 7 中所示，可以引入 IPSec 网关 38，作为网络布局 10 的一部分，以保证原籍网络 12 周边的安全。如图所示，由于使用 IPSec 网关 38 或类似的装置，现在的客户 24 可以直接在它本身与 IPSec 网关 38 之间，建立 IPSec 隧道 40。IPSec 隧道 40 的配置，最好能使来自客户 24 的分组，经过加密链路 42，通向网络 12 的内部前，让 IPSec 网关 38 来鉴证它们。另外，按照本发明的一个优选实施例，可以配置 IPSec

网关 38，引入如上述中继服务器 22 的相同功能。

按照本发明的一个优选实施例，IPSec 网关 38 可以是 VPN 网关或类似的装置。又按照本发明的一个优选实施例，可以用 IPSec ESP 或 AH 协议来鉴证分组。

从上面的详细说明容易明白，本发明的系统和方法，可以用于各种需要网络安全性和移动性的网络配置。本发明的系统和方法还有高度的灵活性且易于修改和定制，以适应特定的情况。例如，本发明可以在各种网络布局内使用，如包括以太网与 Token Ring 接入方法的区域网（LAN）、无线区域网（WLAN）、城域网（MAN）、虚拟区域网（VLAN）、广域网（WAN）、和蓝牙网络。此外，本发明可以在无线数据网络内工作，如 GPRS、NTT DoCoMo、Hot Spots、GSM-Data、CDMA-One、和 HS-CDS 网络，以及布线的公共网络，如 POTS、DSL、Cable 和 ISDN 网络。

还有，虽然各优选实施例的讨论没有指明特定的操作环境，但本发明可以用于各种服务器平台与操作环境，诸如，举例说，Windows NT、Me、XP、95、98、和 2000，以及 Unix、OS/2、Pocket PC、和 NetWare。

此外，本发明可以与各种组网链路和协议一起使用，例如，包括那些基于 Network File System（NFS）；Web NFS；Server Message Block（SMB）；Samba；Netware Core Protocol（NCP）；Distributed File System（DFS）；和 Common Internet File System（CIFS）结构，以及使用诸如 TCP/IP、IPX/SPX、HTTP、HTTPS、及 NetBEUI 这样的传播协议。

已经具体参考各优选实施例，说明了本发明，各优选实施例应认为是示范而不是限制。本领域熟练人员显然知道，还存在不违背本发明的精神和范围，从而属于本发明的另外实施例。因此，本发明的这些变化和修改，可以认为是在下面权利要求书的精神和范围内实现的。

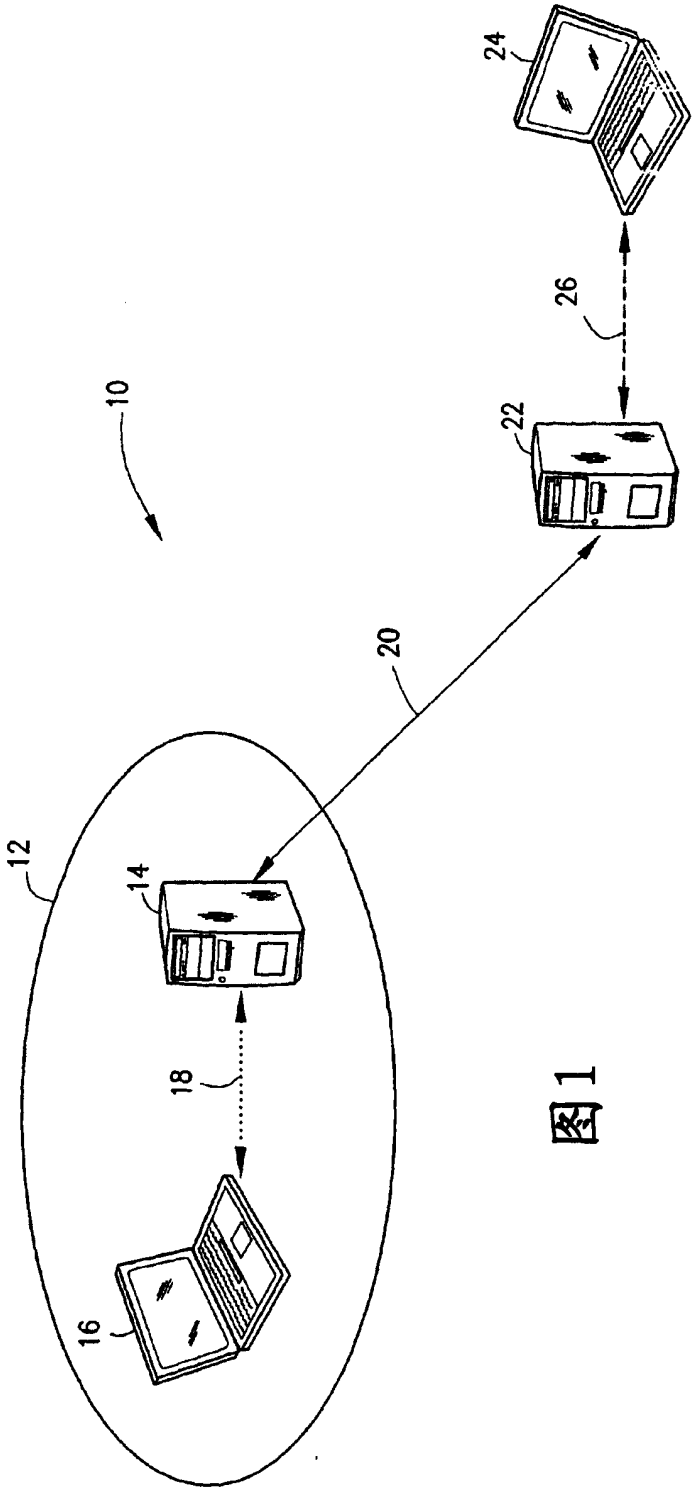


图1

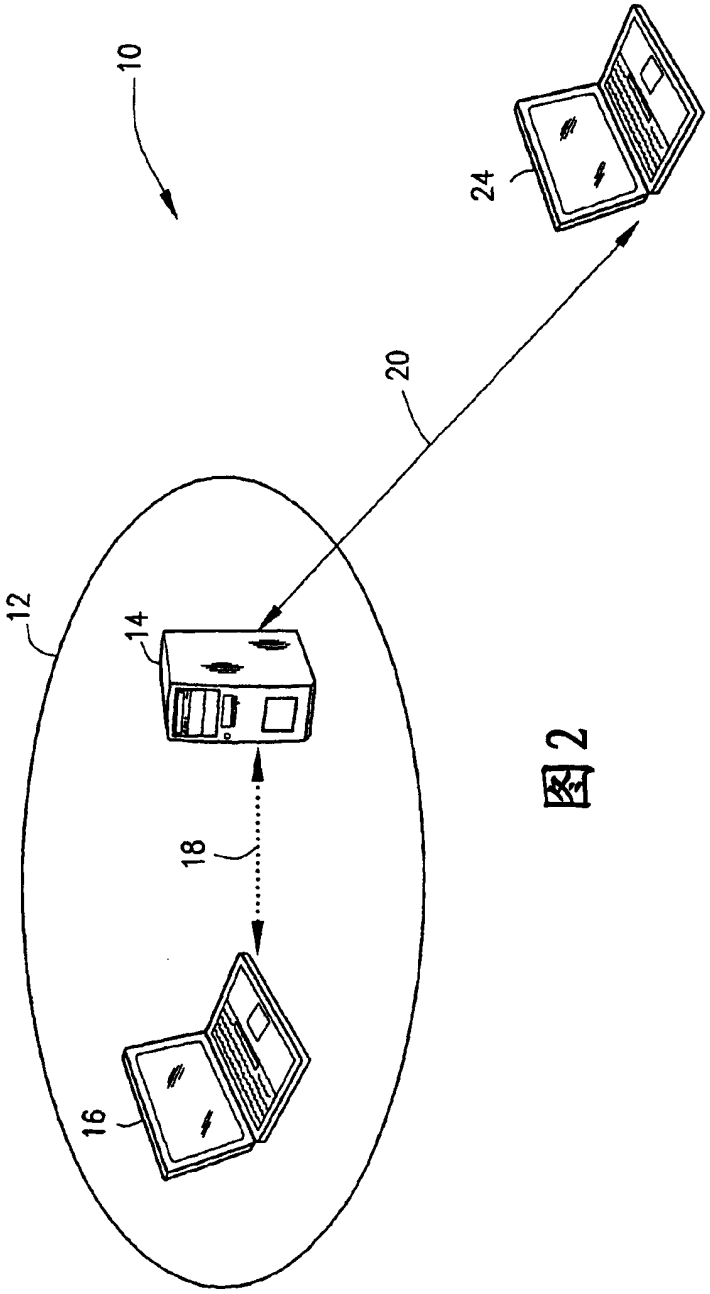


图2

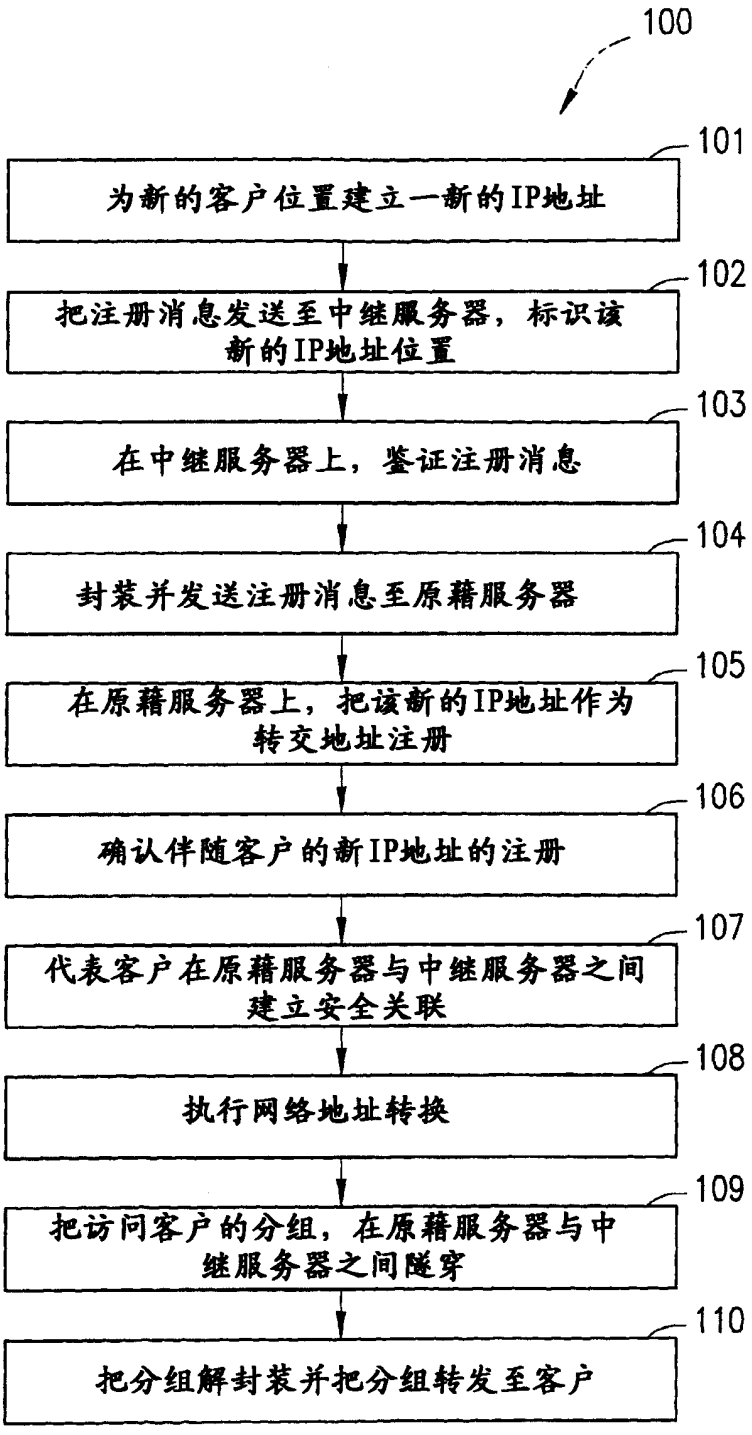
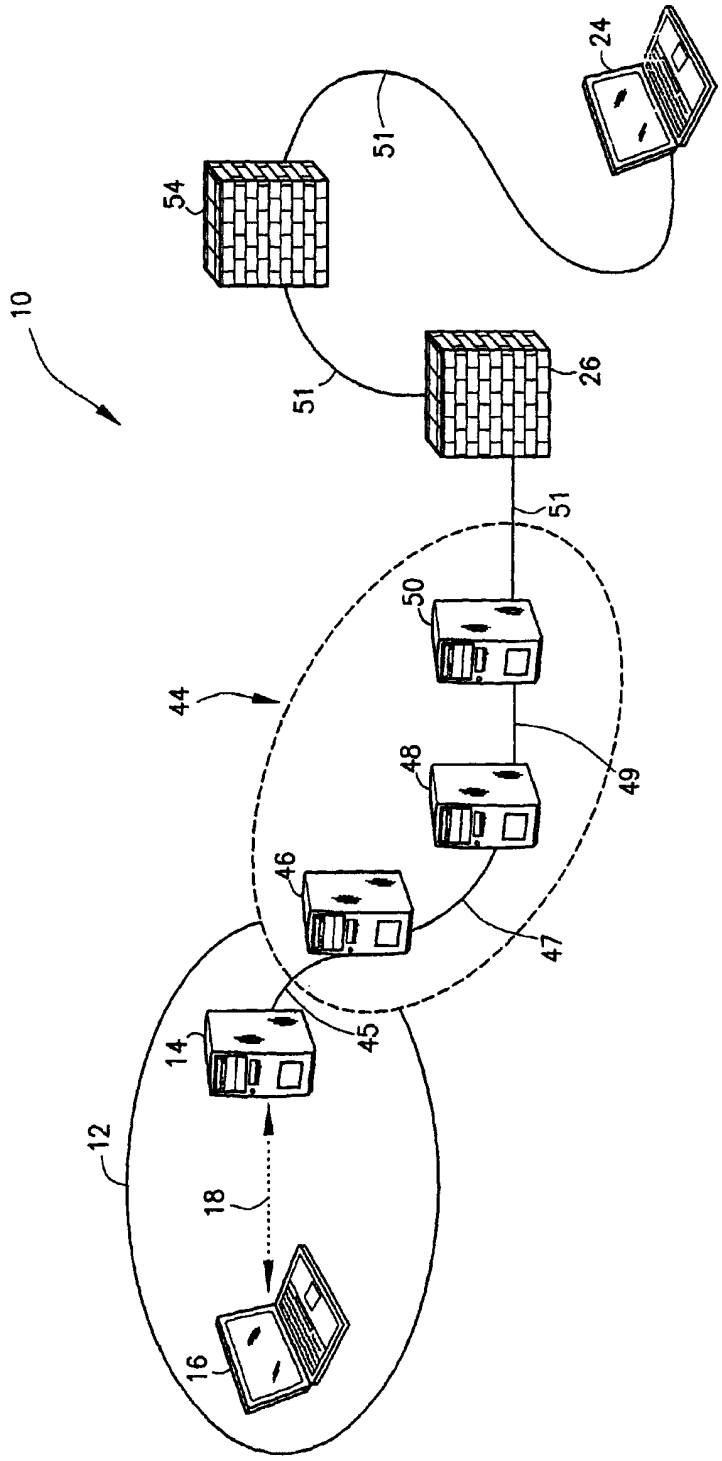

100
101
为新的客户位置建立一新的IP地址
102
把注册消息发送至中继服务器，标识该新的IP地址位置
103
在中继服务器上，鉴证注册消息
104
封装并发送注册消息至原籍服务器
105
在原籍服务器上，把该新的IP地址作为转交地址注册
106
确认伴随客户的新IP地址的注册
107
代表客户在原籍服务器与中继服务器之间建立安全关联
108
执行网络地址转换
109
把访问客户的分组，在原籍服务器与中继服务器之间隧穿
110
把分组解封装并把分组转发至客户

图3



通过HTTP隧道横越防火墙

图 4

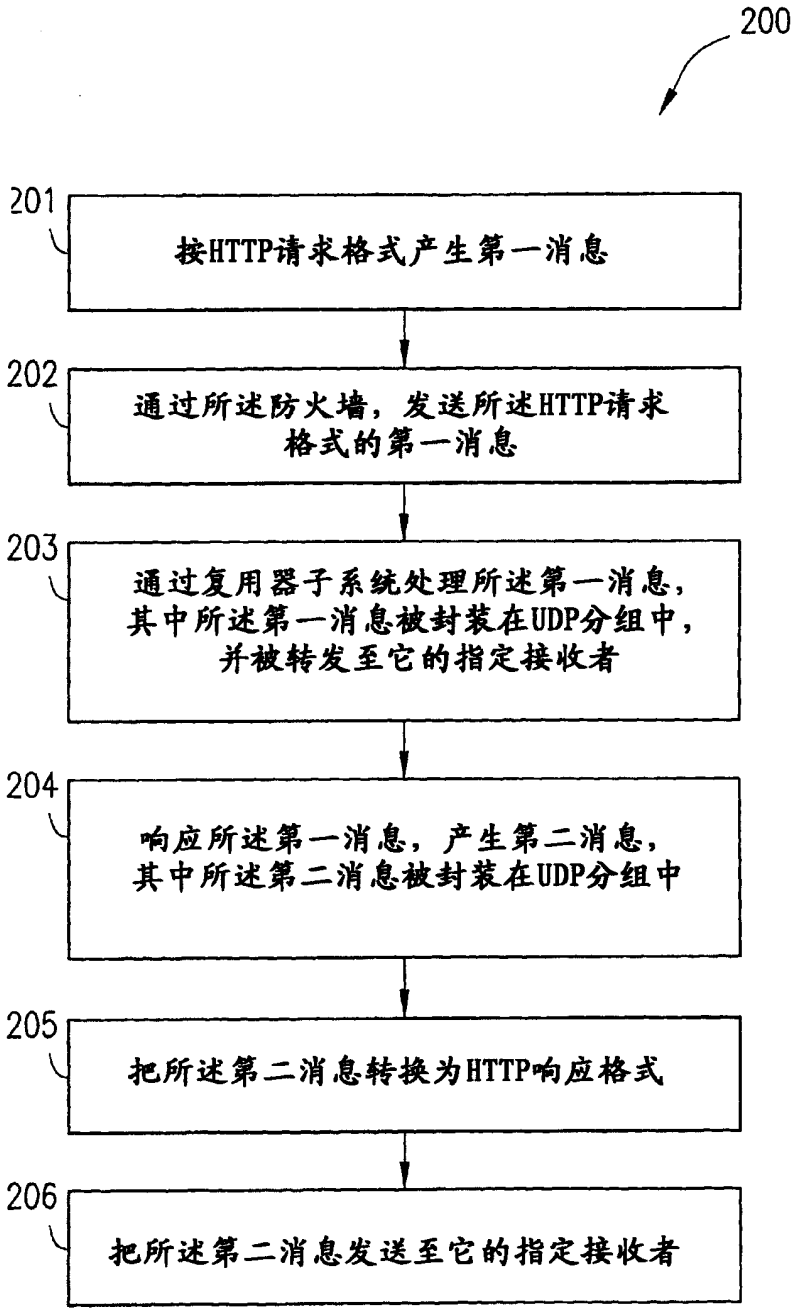

200
201
按HTTP请求格式产生第一消息
202
通过所述防火墙，发送所述HTTP请求格式的第一消息
203
通过复用器子系统处理所述第一消息，其中所述第一消息被封装在UDP分组中，并被转发至它的指定接收者
204
响应所述第一消息，产生第二消息，其中所述第二消息被封装在UDP分组中
205
把所述第二消息转换为HTTP响应格式
206
把所述第二消息发送至它的指定接收者

图5

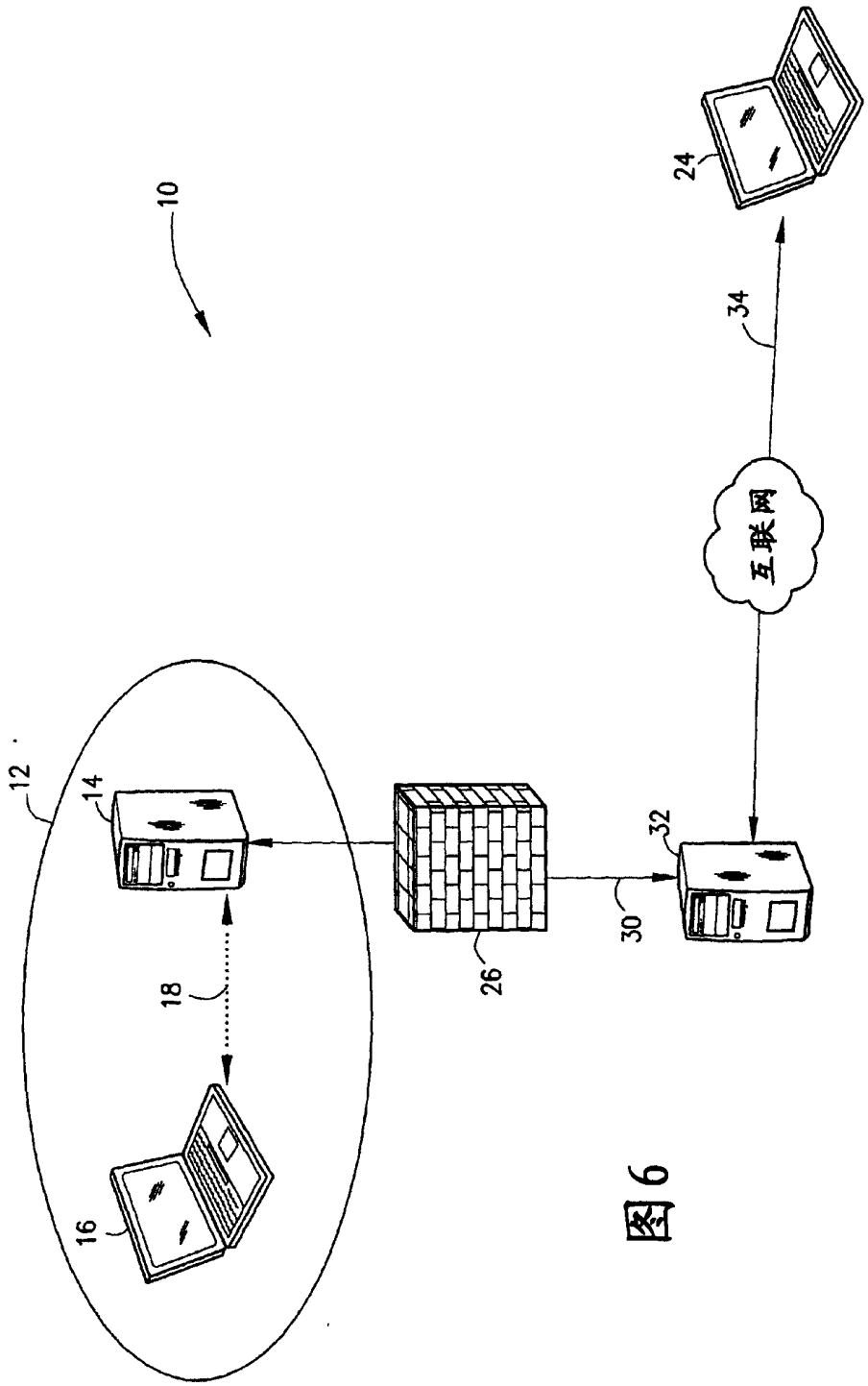


图6

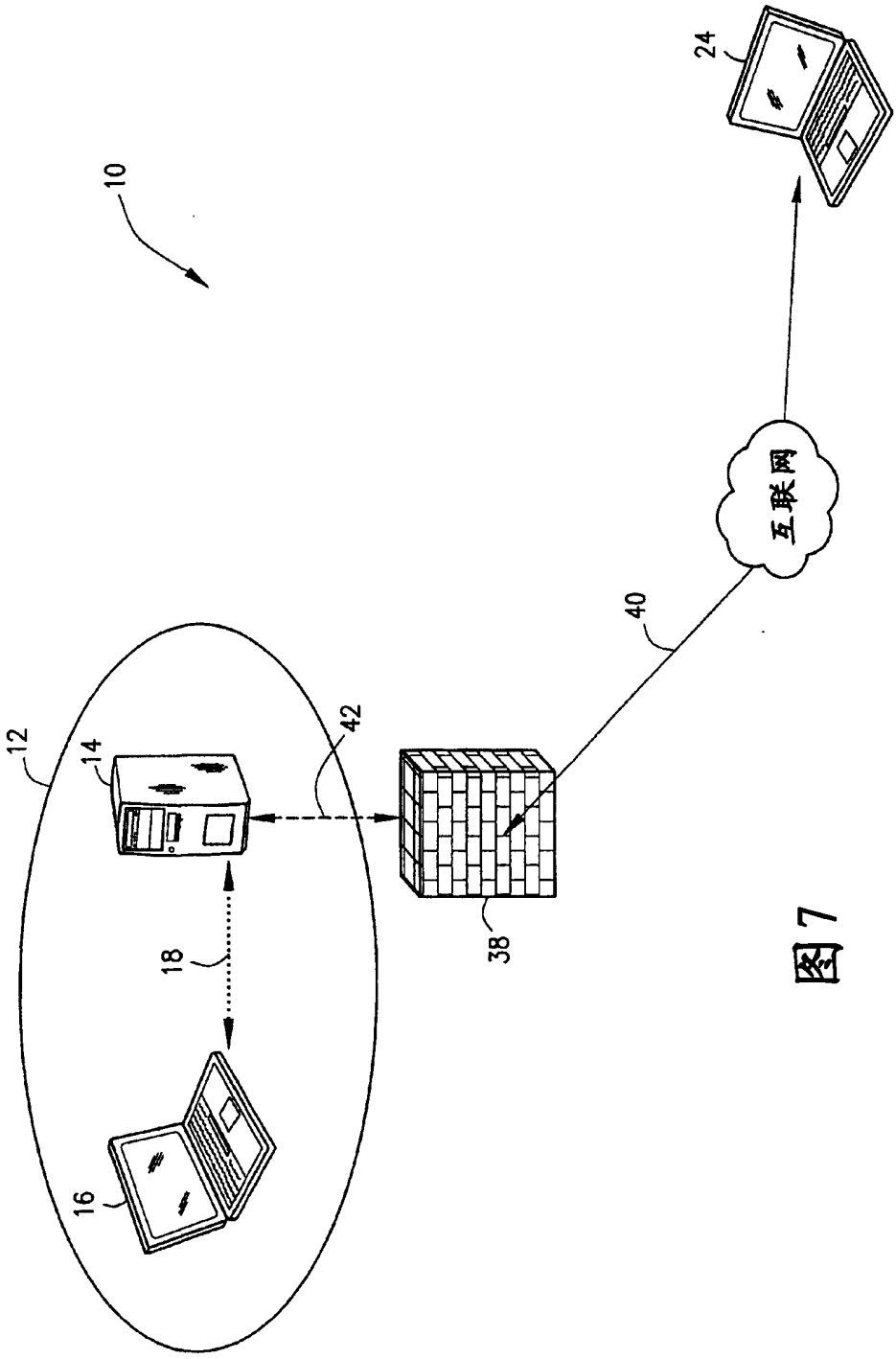


图7