

(12) 发明专利

(10) 授权公告号 CN 101228762 B

(45) 授权公告日 2013. 02. 27

(21) 申请号 200680026629. 7

(56) 对比文件

(22) 申请日 2006. 06. 02

WO 2005/043847 A1, 2005. 05. 12,

(30) 优先权数据

US 2002199114 A1, 2002. 12. 26,

11/144, 966 2005. 06. 03 US

WO 02/067540 A1, 2002. 08. 29,

(85) PCT申请进入国家阶段日

审查员 李晓利

2008. 01. 21

(86) PCT申请的申请数据

PCT/IB2006/001449 2006. 06. 02

(87) PCT申请的公布数据

W02006/129182 EN 2006. 12. 07

(73) 专利权人 诺基亚公司

地址 芬兰埃斯波

(72) 发明人 J·维克芒 F·多萨 S·帕尔科

(74) 专利代理机构 北京市金杜律师事务所

11256

代理人 吴立明

(51) Int. Cl.

H04L 29/02 (2006. 01)

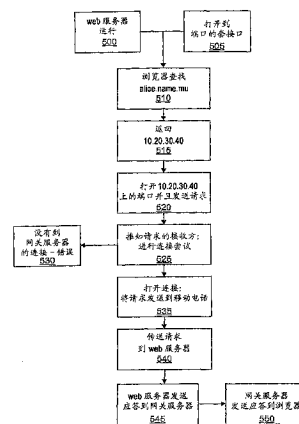
权利要求书 3 页 说明书 5 页 附图 6 页

(54) 发明名称

用于访问居于防火墙之后的具有动态 IP- 地址的 web 设备的系统和方法

(57) 摘要

一种用于提供访问位于防火墙内的电子设备上的 web 服务器的系统和方法。网关设备包括在防火墙之外提供的网关服务器。网关设备包括对应于在 web 服务器的 DNS 名中所使用的同一 DNS 扩展的 IP 地址。当客户端设备尝试通过 DNS 名联系 web 服务器时, 该请求传送到网关服务器, 然后该网关服务器与该 web 服务器进行通信。



1. 一种提供访问居于防火墙之后的移动设备上的 web 服务器的方法,包括:
使得网关服务器位于所述防火墙以外,所述网关服务器拥有对应于预定 DNS 扩展的 IP 地址,其中所述 web 服务器的 DNS 名包括所述预定 DNS 扩展;
当客户端设备尝试使用所述 DNS 名联系所述移动设备时,使得所述网关服务器接收所述联系尝试以及其中所包含的信息;以及
使得所述网关服务器在已经由所述移动设备打开的至该网关服务器的连接上传送包含在所述联系尝试中的信息到所述 web 服务器。
2. 根据权利要求 1 所述的方法,进一步包括:
使得所述网关服务器接收来自所述 web 服务器的响应信息;以及
使得所述网关服务器中继所述响应信息到客户端设备。
3. 根据权利要求 1 所述的方法,进一步包括:
当所述网关服务器接收到所述联系尝试以及其中所包含的信息时,确定所述 web 服务器是否具有与所述网关服务器的打开连接;以及
如果所述 web 服务器不具有与所述网关服务器的打开连接,则传送错误应答到所述客户端设备。
4. 根据权利要求 1 所述的方法,其中所述网关服务器和所述 web 服务器通过指定端口进行通信,该指定端口与所述客户端设备用于与所述网关服务器进行通信的端口相分立。
5. 根据权利要求 1 所述的方法,在使得所述网关服务器传送包含在到所述 web 服务器的联系尝试中的信息之前,进一步包括:
使得所述移动设备尝试使用 web 端口打开与所述网关服务器之间的套接口,
如果所述移动设备不能打开所述套接口,则使得所述移动设备打开到所述网关服务器的 HTTP 连接,
使用特定 URL 将 HTTP 请求从所述移动设备传送到所述网关服务器;
使得所述网关服务器使用附加端口创建附加传入套接口;
将所述附加端口的编号通知给所述移动设备;
使得所述移动设备尝试使用所述附加端口打开与所述网关服务器之间的套接口;以及
继续使得所述移动设备尝试使用附加端口打开与所述网关服务器的套接口直到尝试成功。
6. 一种用于提供通过防火墙访问 web 服务器的系统,包括:
移动设备,位于所述防火墙之后并且该移动设备包括所述 web 服务器,所述 web 服务器拥有具有预定 DNS 扩展的 DNS 名;以及
网关设备,位于所述防火墙之外并且该网关设备包括网关服务器,所述网关服务器具有对应于所述 DNS 扩展的 IP 地址,
其中,当客户端设备尝试使用所述 DNS 名联系所述移动设备时,所述网关服务器接收所述联系尝试以及其中所包含的信息,所述网关服务器在已经由所述移动设备打开的至该网关服务器的连接上将包括在所述联系尝试中的信息传送到所述 web 服务器。
7. 根据权利要求 6 所述的系统,其中所述网关服务器接收来自所述 web 服务器的响应信息并且将所述响应信息中继到所述客户端设备。
8. 根据权利要求 6 所述的系统,其中所述网关服务器和所述 web 服务器通过指定端口

进行通信,该指定端口与所述客户端设备用于与所述网关服务器进行通信的端口相分立。

9. 根据权利要求 6 所述的系统,其中当所述网关服务器接收到所述联系尝试以及其中所包含的信息时,所述网关服务器确定所述 web 服务器是否具有与所述网关服务器的打开连接,并且如果不存在打开的连接则向所述客户端设备传送错误应答。

10. 一种用于提供通过防火墙访问 web 服务器的装置,包括:

用于提供网关设备上的网关服务器的装置,所述网关服务器具有对应于 DNS 扩展的 IP 地址;

用于接收来自客户端设备的针对所述防火墙之后的移动设备的联系尝试的装置,所述移动设备具有包括所述 DNS 扩展的 DNS 名;以及

用于在已经由所述移动设备打开的至该网关服务器的连接上将包括在所述联系尝试中的信息传送到所述移动设备上的所述 web 服务器的装置。

11. 根据权利要求 10 所述的装置,进一步包括:

用于接收来自所述 web 服务器的响应信息的装置;以及

用于中继所述响应信息到所述客户端设备的装置。

12. 根据权利要求 10 所述的装置,进一步包括:

用于在接收到所述联系尝试以及其中所包含的信息之后,确定所述 web 服务器是否具有与所述网关服务器的打开连接的装置;以及

用于如果所述 web 服务器不具有与所述网关服务器的打开连接,则向所述客户端设备传输错误应答的装置。

13. 根据权利要求 10 所述的装置,其中所述网关服务器和所述 web 服务器通过指定端口进行通信,所述指定端口与所述客户端设备用于与所述网关服务器进行通信的端口相分立。

14. 一种用于支持与防火墙外的客户端设备进行通信的设备,包括:

用于提供移动设备上的 web 服务器的装置;

用于向所述移动设备分配具有预定 DNS 扩展的 DNS 名的装置,所述 DNS 扩展对应于用于防火墙之外的网关服务器的 IP 地址,其中所述移动设备位于所述防火墙之内;

用于接收包括在来自所述防火墙之外的客户端设备的联系尝试中的信息的装置,所述信息通过所述网关服务器在已经由所述移动设备打开的至该网关服务器的连接上被传送到所述 web 服务器。

15. 根据权利要求 14 所述的设备,进一步包括用于将响应信息传送到所述网关服务器的装置,所述网关服务器中继所述响应信息到所述客户端设备。

16. 根据权利要求 14 所述的设备,其中所述网关服务器和所述 web 服务器通过指定端口进行通信,所述指定端口与所述客户端设备用于与所述网关服务器进行通信的端口相分立。

17. 根据权利要求 14 所述的设备,进一步包括:

用于尝试使用 web 端口打开从所述移动设备的与所述网关服务器之间的套接口的装置;

用于如果所述移动设备不能打开所述套接口,则如下进行操作的装置:

打开从所述移动设备到所述网关服务器的 HTTP 连接,

使用特定 URL 将 HTTP 请求从所述移动设备传送到所述网关服务器 ; 以及
当接收到响应于所述 HTTP 请求的来自所述网关服务器的附加端口的编号时, 尝试使用所述附加端口打开从所述移动设备的与所述网关服务器之间的套接口 ; 以及
用于继续尝试使用附加端口打开从所述移动设备的与所述网关设备的套接口直到尝试成功的装置。

用于访问居于防火墙之后的具有动态 IP- 地址的 web 设备的系统和方法

技术领域

[0001] 本发明总体涉及移动电子设备上的 web 服务器。更具体地,本发明涉及访问位于防火墙之后的移动电子设备上的 web 服务器。

[0002] 背景技术

[0003] 目前,用于移动设备诸如移动电话的网络连接性由运营商来提供。网络连接性可以包涉及系统的使用,使得通用分组无线业务(GPRS)允许跨移动电话网络发送和接收信息。可能期望一种置于该移动设备之上的服务器,其中该服务器可由在因特网上的设备上运行的客户端访问。

[0004] 然而在这种系统中,目前存在多种障碍必须加以克服。在当前的运营商网络中,对移动设备分配临时网际协议(IP)地址。因此,尝试访问在这种设备上的 web 服务器的客户端设备必须提供有一种到达该服务器的方式,该方式独立于已经分配给移动设备的 IP 地址。这构成了这种系统中的基本可访问能力问题。

[0005] 然而,即使具有内置服务器的移动设备被分配静态 IP 地址,或者如果使用了诸如动态域名系统(DNS)的技术,该服务器将仍是不可访问的。这是由于以下事实:运营商防火墙通常不允许创建从因特网上的设备到运营商网络内的移动设备的连接。作为代替的是,必须创建从运营商网络的内部出发并且向外延伸到客户端设备的连接。

[0006] 尽管已经尝试解决这个可访问能力的问题,但是这些所提出的解决方案中的每个都具有严重的缺陷。一个提出的解决方案涉及端口碰撞。通过端口碰撞,当某些防火墙端口编号在“秘密”序列中碰撞时,则一个特定端口编号被打开一小段时间。这个概念在 www.linuxjournal.com/article.php?sid=6811 中有讨论。另一解决方案涉及使用防火墙控制协议(FCP),其可以支持第三、信任方动态地控制防火墙(即打开哪些端口,端口被打开的时间段,允许哪些客户端具有打开的端口等等)。FCP 在 www.iptel.org/fcp/ietf-fcp.ppt 中有讨论。然而,对于这两种系统,要求至少给予网络外的设备某种对防火墙的间接控制。为了满足这一要求,运营商将需要在它们的基础设施中投资更多并且可能尝试解决目前还没有的工业标准的问题。而且使防火墙动态可配置还将导致需要修改 web 浏览器,这是不希望发生的。

[0007] 除此之外,即使拥有服务器的移动设备和从该服务器进行访问的设备处于同一运营商网络中,即使客户端知道临时 IP 地址,仍不存在该服务器可被访问的保证。特别地,典型运营商通常不直接在移动设备之间现时路由分组。

发明内容

[0008] 本发明通过引入网关解决上述问题,该网关从因特网上的客户端设备向诸如移动电话的移动设备上的 web 服务器透明地传递请求。类似地,该网关从移动 web 服务器应答发起该请求的客户端。

[0009] 本发明的系统和方法提供了高于传统系统的多个优点。本发明允许在当前存在的

运营商网络中访问诸如移动电话的移动设备上的 web 服务器,而不要求来自相应设备的运营商的任何参与。附加地,本发明允许诸如移动电话的设备成为因特网的正式成员,不必等待移动 IPv6 协议变为可用。

[0010] 根据结合附图的下述详细描述,本发明的这些和其他目的、优势以及特征,与本发明的操作方式和组织将一并变得明显,其中类似元素在贯穿下文中描述的多个附图具有类似标号。

附图说明

[0011] 图 1 是根据本发明的实施方式的系统的概观示图;

[0012] 图 2 是可以用于本发明实施的移动电话的透视图;

[0013] 图 3 是图 2 中的移动电话的电话电路的示意性表示;

[0014] 图 4 是根据本发明的一个实施方式的简化移动设备、客户端设备以及网关计算机 / 网关服务器的表示;

[0015] 图 5 是示出了根据本发明的一个实施方式实施的流程图;以及

[0016] 图 6 是示出了在运营商阻碍待使用特定端口的事件中打开客户端设备和网关计算机之间的套接口的过程的流程图。

具体实施方式

[0017] 图 1 示出了在其中可以使用本发明的系统 10,该系统包括可以通过网络进行通信的多个通信设备。系统 10 可以包括有线网络或者无线网络的任何组合,其中无线网络包括,但不限于移动电话网络、无线局域网 (LAN)、蓝牙个人局域网、以太网 LAN、令牌环 LAN、广域网、因特网等等。系统 10 可以包括有线通信设备和无线通信设备两者。

[0018] 作为示例,图 1 中的所示的系统 10 包括移动电话网 11 和因特网 28。到因特网 28 的连接性可以包括,但不限于远程无线连接、短距离无线连接以及各种无线连接,包括但不限于,电话线、电缆、电源线等等。

[0019] 系统 10 的示例性通信设备可以包括,但不限于移动电话 12、PDA 和移动电话的组合 14、PDA 16、集成消息收发设备 (IMD) 18、台式计算机 20 以及笔记本电脑 22。通信设备可以固定,或者当通信设备由正在移动的个人携带时,该通信设备可以是移动的。通信设备还可以位于以下运输模式中,该传输模式包括但不限于,汽车、卡车、出租车、公共汽车、船舶、飞机、自行车、摩托车等等。其中一些或者所有通信设备可以向基站 24 发送和接收呼叫和消息并且可以通过无线连接 25 与服务供应商进行通信到基站 24。基站 24 可以连接到网络服务器 26,该网络服务器 26 允许移动电话网 11 和因特网 28 之间的通信。系统 10 可以包括附加的通信设备和不同类型的通信设备。

[0020] 通信设备可以使用各种传输技术来进行通信,其中包括但不限于,码分多址 (CDMA)、移动通信全球系统 (GSM)、全球移动通信系统 (UMTS)、时分多址 (TDMA)、频分多址 (FDMA)、传输控制协议 / 网际协议 (TCP/IP)、短消息收发服务 (SMS)、多媒体消息收发服务 (MMS)、电子邮件、即时消息收发服务 (IMS)、蓝牙、IEEE 802.11 等。通信设备可以使用各种媒体进行通信,包括但不限于,无线电、红外、激光、电缆连接等等。

[0021] 图 2 和图 3 示出了根据本发明的一个实施方式的一个代表性移动电话 12。然而,

应该理解到本发明并不旨在限于一种特定类型的移动电话 12 或者其他电子设备。图 2 和图 3 的移动电话 12 包括外壳 30、液晶显示器形式的显示器 32、小键盘 34、麦克风 36、耳机 38、电池 40、红外端口 42、天线 44、根据本发明的一个实施方式的 UICC 形式的智能卡 46、读卡器 48、无线接口电路 52、编解码器电路 54、控制器 56 以及存储器 58。各电路和元件是现有技术中已知的所有类型，例如在 Nokia 移动电话范畴内。

[0022] 在图 4 中以简化形式示出的本发明在以下情形下操作，其中不具有固定 IP 地址的移动设备 100 居于运营商防火墙之后。防火墙防止创建从网络外部到移动设备 100 的连接，而是仅允许从移动设备 100 到网络外部创建连接。本发明解决了以下情形下的问题，其中 web 服务器 110 在移动设备上运行，并且希望对于因特网 28 上的至少一个客户端设备 120（移动设备和 / 或固定设备两种）而言服务器 100 是可访问的。

[0023] 根据本发明，在因特网上的客户端设备 120 和移动设备 100 上的 web 服务器 110 之间的通信中所使用的协议如下：当由客户端设备 120 将请求发送到 web 服务器 110 时，该请求包含关于电子设备 100 意图请求的信息。网关计算机 130 仍建立在运营商防火墙之外，因特网上的某处。网关计算机 130 包括在两个端口上侦听的网关服务器 140。对于因特网 28 上的客户端设备 120 而言一个端口（HTTP 端口）是已知的，则该端口称为指定端口。客户端设备 120、移动设备 100 和网关计算机 130 都可以拥有图 3 中所示的电路类型和功能性类型。

[0024] 包含 web 服务器 110 的移动设备 100 进行到打开对网关服务器 140 的指定端口的连接。对每个移动设备 100 分配名称并且将其布置使得 DNS 查找该名称带来网关计算机 130 的 IP 地址得以返回。网关服务器 140 寻找从各种客户端设备 120 到已知端口所到达的每个请求，并且使用该内容以便推知移动设备 100 意图的请求。然后网关服务器 140 在由移动设备 100 打开的连接上传递该请求。移动设备 100 上的 Web 服务器 110 随即在同一连接上返回应答，并且将该应答传送到客户端设备 120。在此过程中，看起来好像移动设备 100 上的 web 服务器 110 从因特网上的任何客户端设备 120 直接可访问。这样，移动设备 100 已经变为可寻址并且可访问。

[0025] 本发明的实施通常如下所述并且如图 5 中所示。在此特定的实施中，移动设备 100 包括移动电话，并且协议是 HTTP。在此实施中，DNS 被配置为所有 DNS 查找特定扩展中的结尾，诸如“name.mu”，得到网关计算机的 IP 地址。仅出于说明的目的，假设 IP 地址是 10.20.30.40。在实践中，这意味着查找诸如 alice.name.mu 和 bob.name.mu 得到 IP 地址 10.20.30.40。

[0026] 如前所述，网关计算机 130 包括网关服务器 140，该网关服务器侦听通用 HTTP 端口 80 以及例如端口 2050。在移动电话上，在步骤 500，web 服务器 110 开始运行，并且其侦听通常的 HTTP 端口 80。然而，由于上述问题，所以此 web 服务器 110 对于移动电话外部的任何设备不可访问。而且，运行另一过程，在此称为连接者。在步骤 505，连接者打开到端口 2050 的套接口。作为打开该套接口的一部分，连接者声明移动电话的标识。作为此打开序列的一部分，网关服务器 140 知晓移动电话的名称。在此示例中，移动电话称为“alice.”。

[0027] 在因特网上的某人尝试浏览 alice.name.mu 的事件中，发生以下系列事件。在步骤 510，客户端设备 120 上的浏览器执行查找 alice.name.mu。在步骤 515，此查找返回 10.20.30.40 作为网关服务器 140 的 IP 地址的结果。在步骤 520，浏览器进行到

10. 20. 30. 40 上的 HTTP 端口 80 并且传送常规 HTTP 请求。HTTP 请求报头在其头字段中包括 `alice.name.mu`。

[0028] 在步骤 525, 根据头字段的值, 网关服务器推知对于请求的接收方。如果名为 `alice` 的设备已经打开到网关服务器 140 的连接, 则在步骤 535, 网关服务器 140 在该连接上发送请求到移动电话。如果移动电话没打开到网关服务器的连接, 则在步骤 530, 网关服务器 140 以适合的错误应答做出响应。当该请求到达移动电话上的连接者时, 在步骤 540, 连接者将其传送到在移动电话上运行的 web 服务器 110。当 web 服务器应答时, 在步骤 545 连接者将应答发送回网关服务器。然后在步骤 550 网关服务器进行将其发送回做出初始请求的浏览器。因此, 对于使用浏览器的个体而言, 看起来好像使用 url `alice.name.mu`。可直接访问移动电话。

[0029] 图 5 中所示的解决方案依赖于移动设备 100 能够打开从移动设备 100 到网关服务器 140 的 TCP/IP 套接口。然而, 运营商可以通过阻碍在移动设备 100 和网关计算机 130 之间的通信中所使用的端口来防止发生此创建。图 6 是示出了根据本发明的一个实施方式解决此问题的处理的流程图。在此处理中, 假设运营商不阻碍每个潜在端口, 并且运营商不阻碍端口 80。

[0030] 如图 6 中所示, 在步骤 600 移动设备 100 尝试打开到网关服务器 140 的套接口。如果其尝试成功, 则不需要附加动作并且如上所述地进行图 5 中的处理。其在步骤 610 中表示。如果该尝试失败, 这可能由于运营商在其防火墙中已经阻碍了所期望的端口的事实。作为响应, 在步骤 620, 移动设备 100 使用常规 web 端口 80 打开了到网关计算机 130 的 HTTP 连接。这个步骤很可能成功, 因为运营商阻碍此端口是极不可能的。在步骤 630, 移动设备 100 传送使用特定 URL 的 HTTP 请求并且通知网关服务器 140 不能再使用特定端口。在步骤 640, 网关服务器 140 使用不同的端口创建另一传入套接口并且, 在 HTTP 应答中通知移动设备 100 端口号。然后重复此过程直到找到打开端口, 此时套接口是打开的。即使是可能的, 该系统也使得其很困难, 因为运营商要防止实施本发明的解决方案的连接, 除非阻碍了所有端口, 除非在每个连接上执行业务量分析, 否则其将无目的地给予 2G 和 3G 网络。

[0031] 本发明在方法步骤的常用环境中进行描述, 其可以通过程序产品在一个实施方式中实施, 该程序产品包括可由网络互连环境中的计算机执行的计算机可执行指令, 诸如程序代码。

[0032] 通常地, 程序模块包括例行程序、程序、对象、组件、数据结构等等, 其可以执行特定任务或者实施特定抽象数据类型。与数据结构相关联的计算机可执行指令、以及程序模块表示用于执行在此公开的方法步骤的程序代码的示例。这种可执行指令的特定序列或者相关联的数据结构表示用于实施这些步骤中所描述的功能相对应的动作的示例。

[0033] 本发明的软件和 web 实施可以用标准程序技术来完成, 用基于规则的逻辑、以及其他逻辑来完成各种数据库搜索步骤、关联步骤、对比步骤以及决定步骤。还应该注意在此所使用的和在权利要求书中所使用的词语“组件”和“模块”旨在包括使用一个或者多个软件代码线路的实施, 和 / 或硬件实施、和 / 或用于接收手动输入的设备。

[0034] 为了示意和描述的目的已经进行了对本发明的实施方式的上述描述。不意在穷举或者将本发明限于所公开的精确形式, 并且可以从上述教导或者从本发明的实践获取修改和变形。选择了实施方式并对其进行了描述是为了解释本发明的原理, 以及其实际应用使

得本领域技术人员能够在各种实施方式中利用本发明,以及具有各种适合于特定使用所期望的各种修改。

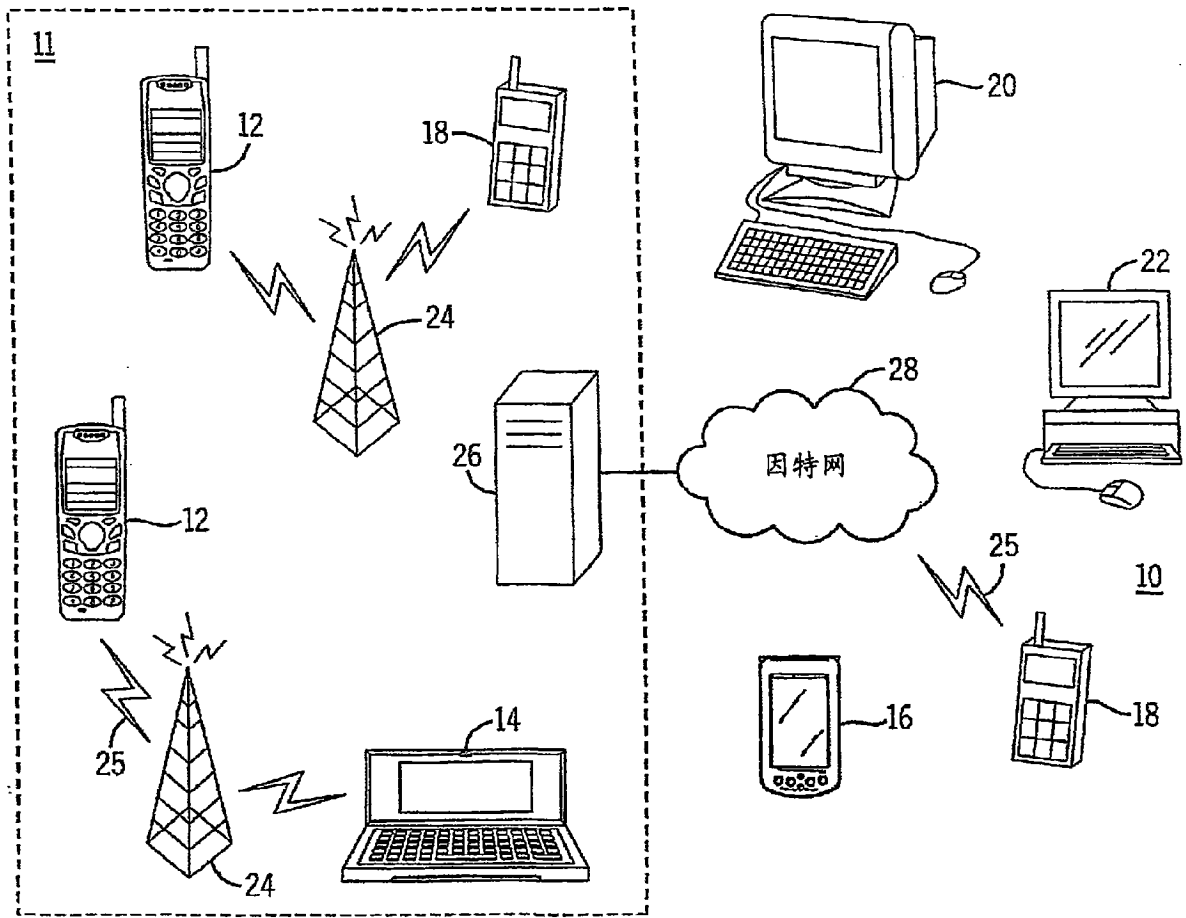


图 1

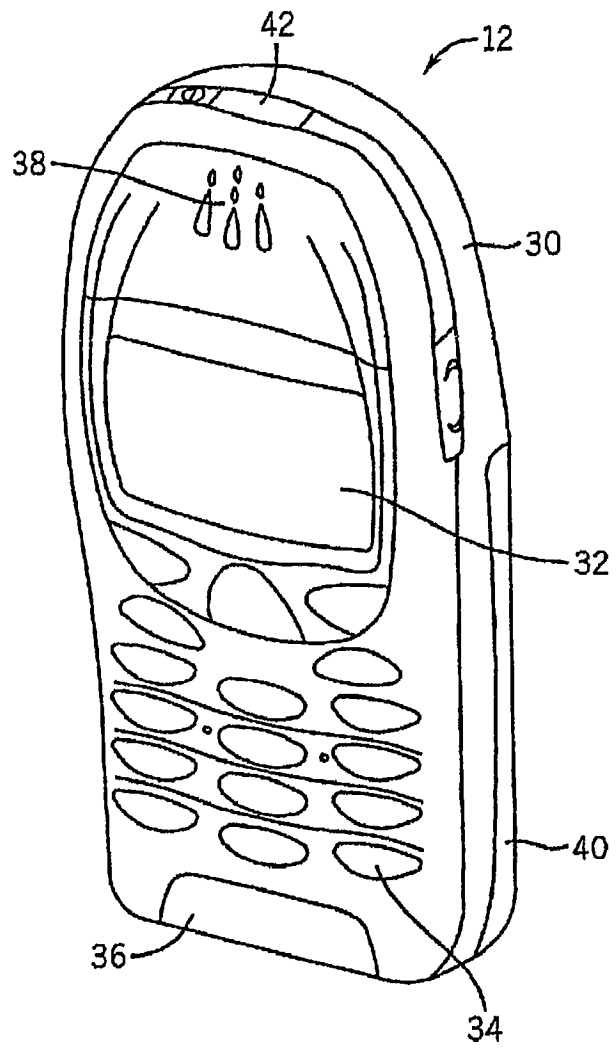


图 2

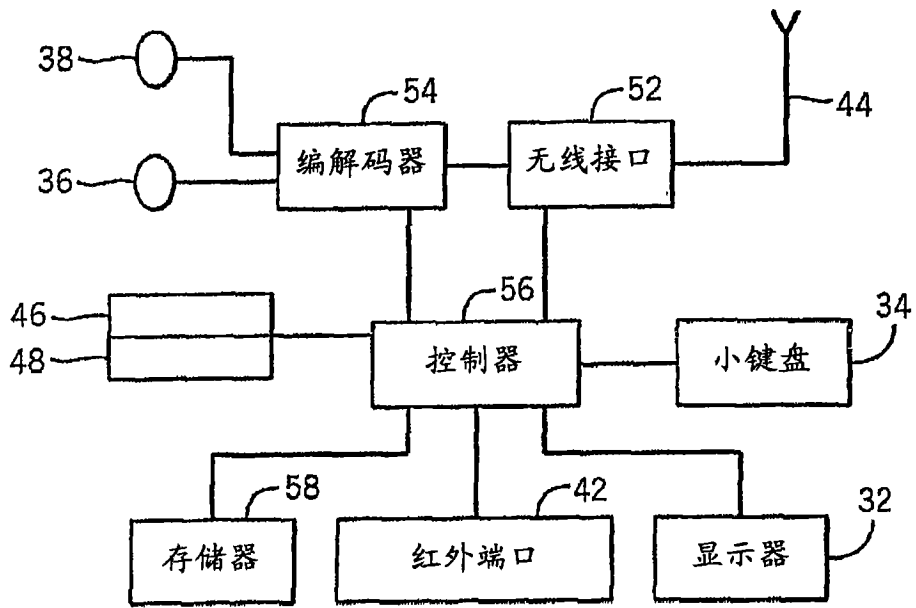


图 3

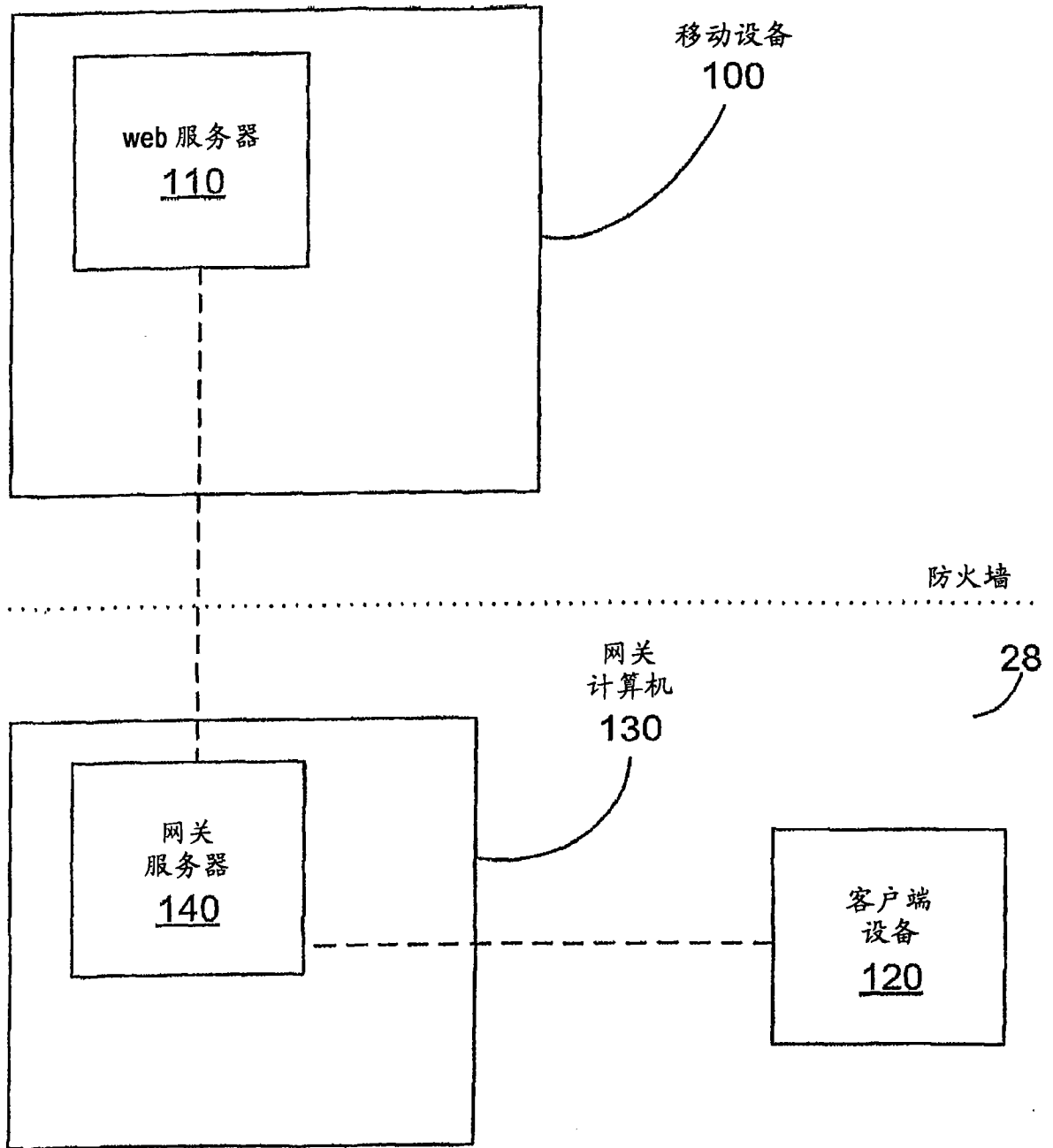


图 4

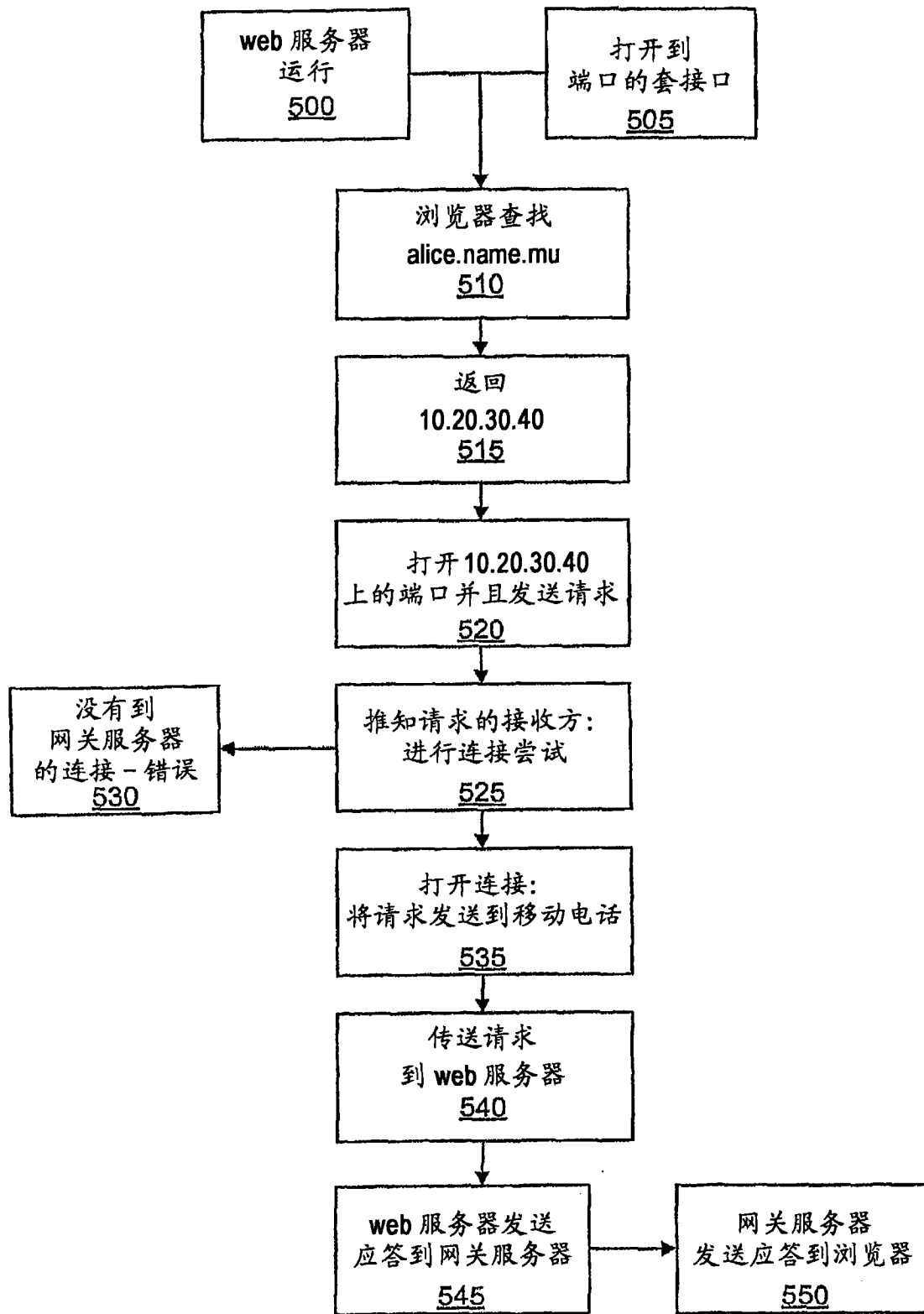


图 5

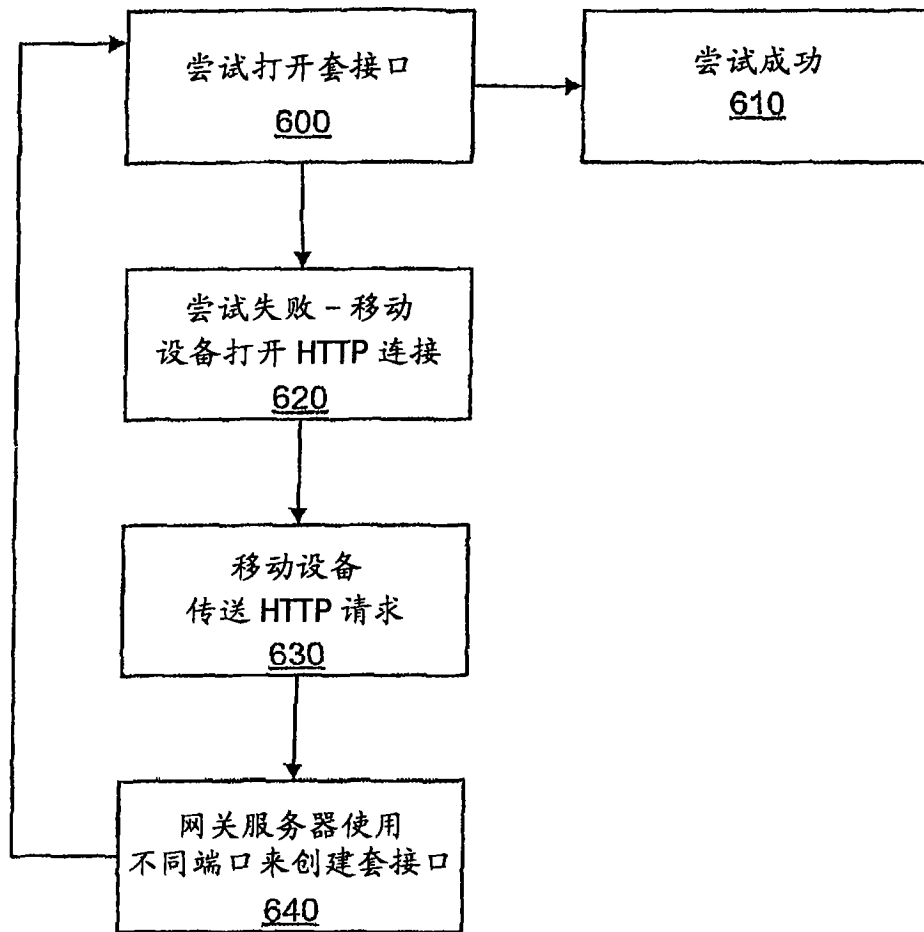


图 6