



# [12] 发明专利说明书

专利号 ZL 200580015167.4

[45] 授权公告日 2009 年 11 月 18 日

[11] 授权公告号 CN 100561499C

[22] 申请日 2005.5.10

[21] 申请号 200580015167.4

[30] 优先权

[32] 2004.5.13 [33] US [31] 60/570,999

[32] 2004.6.9 [33] US [31] 10/866,506

[32] 2004.6.9 [33] US [31] 10/866,507

[32] 2004.6.9 [33] US [31] 10/866,285

[32] 2005.4.11 [33] US [31] 11/104,140

[86] 国际申请 PCT/US2005/016484 2005.5.10

[87] 国际公布 WO2005/114545 英 2005.12.1

[85] 进入国家阶段日期 2006.11.13

[73] 专利权人 思科技术公司

地址 美国加利福尼亚州

[72] 发明人 亚瑟·G·霍瓦瑟 拉尔夫·多莫斯  
罗兰·萨威勒 劳伦斯·克里格

克里斯多佛·韦伯尔

威卡斯·布塔尼 拉吉·辛加尔

加里·丹尼斯·小沃格特

[56] 参考文献

WO2004003801A1 2004.1.8

US5887176A 1999.3.23

CN1479908A 2004.3.3

CN1307706A 2001.8.8

CN1349639A 2002.5.15

US5850187A 1998.12.15

审查员 李秀改

[74] 专利代理机构 北京东方亿思知识产权代理有  
限责任公司

代理人 李晓冬

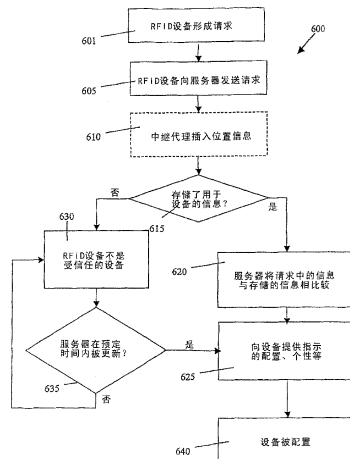
权利要求书 4 页 说明书 28 页 附图 16 页

[54] 发明名称

定位和供给 RFID 设备的方法和设备及相关网络  
网络设备

[57] 摘要

提供了用于请求(601)、识别、定位(610)、配置(640)和供给网络中的设备的方法和设备。根据本发明的一些实现方式,MAC 地址信息和 EPC 信息可被组合,以标识特定设备及其在网络中的位置。对于使用动态主机配置协议(“DHCP”)的实现方式,DHCP 选项可被用于传递供给和其他信息。一些实现方式采用域名服务(“DNS”)和动态 DNS(“DDNS”)来允许容易地识别设备。



1. 一种用于唯一地供给射频识别设备的方法，所述方法包括：  
在网络上接收供给请求；  
根据被包括在所述供给请求中的电子产品代码和介质访问控制地址，  
自动识别射频识别设备；以及  
根据被包括在所述供给请求中的位置信息，自动定位所述射频识别设备。
2. 如权利要求 1 所述的方法，还包括以下步骤：在所述射频识别设备被定位之后，自动发起重供给周期，以向所述射频识别设备提供不同的功能。
3. 如权利要求 1 所述的方法，还包括在自动定位所述射频识别设备之后：  
确定先前是否已为所述射频识别设备确立了供给信息；以及  
当确定出先前已为所述射频识别设备确立了供给信息时，供给所述射频识别设备。
4. 如权利要求 1 所述的方法，还包括在自动定位所述射频识别设备之前：  
确定先前是否已为所述射频识别设备确立了供给信息；以及  
当确定出先前已为所述射频识别设备确立了供给信息时，供给所述射频识别设备。
5. 一种用于唯一地供给射频识别设备的方法，所述方法包括：  
形成 DHCPDISCOVER 请求，所述 DHCPDISCOVER 请求包括射频识别设备的电子产品代码和指示所述射频识别设备的位置的位置信息；  
将所述 DHCPDISCOVER 请求发送到动态主机配置协议服务器；以及  
接收来自所述动态主机配置协议服务器的专门针对所述射频识别设备的供给信息。
6. 如权利要求 5 所述的方法，还包括在接收来自所述动态主机配置协议服务器的专门针对所述射频识别设备的供给信息之后，向所述动态主机

配置协议服务器发送 DHCPINFORM 请求的步骤，所述 DHCPINFORM 请求指示所述射频识别设备的当前被使能的功能。

7. 如权利要求 5 所述的方法，还包括在接收来自所述动态主机配置协议服务器的专门针对所述射频识别设备的供给信息之前，向所述动态主机配置协议服务器发送 DHCPINFORM 请求的步骤，所述 DHCPINFORM 请求指示所述射频识别设备的当前被使能的功能。

8. 一种射频识别网络，包括：

用于形成 DHCPDISCOVER 请求的装置，所述 DHCPDISCOVER 请求包括射频识别设备的电子产品代码和指示所述射频识别设备的位置的位置信息；

用于将所述 DHCPDISCOVER 请求发送到动态主机配置协议服务器并且用于接收来自所述动态主机配置协议服务器的为所述射频识别设备专门定制的供给信息的装置。

9. 如权利要求 8 所述的射频识别网络，还包括用于向所述动态主机配置协议服务器发送 DHCPINFORM 请求的装置，所述 DHCPINFORM 请求指示所述射频识别设备的当前被使能的功能。

10. 如权利要求 8 所述的射频识别网络，其中，所述用于形成 DHCPDISCOVER 请求的装置包括用于将所述电子产品代码包括在所述 DHCPDISCOVER 请求中的射频识别设备，和用于将所述位置信息包括在所述 DHCPDISCOVER 请求中的中继代理。

11. 一种网络设备，包括：

用于在网络上接收供给请求的装置；以及

用于根据包括在所述供给请求中的电子产品代码和介质访问控制地址来自动识别射频识别设备，并用于根据包括在所述供给请求中的位置信息定位所述射频识别设备的装置。

12. 如权利要求 11 所述的网络设备，还包括用于发起重供给周期以向所述射频识别设备提供不同的功能的装置。

13. 如权利要求 11 所述的网络设备，还包括用于当确定出先前已为所述射频识别设备确立了供给信息时，控制所述网络设备以供给所述射频识

别设备的装置。

14. 一种用于在网络中部署被唯一地供给的射频识别设备的方法，所述方法包括：

形成 DHCPDISCOVER 请求，所述 DHCPDISCOVER 请求包括射频识别读取器的电子产品代码和指示所述射频识别读取器被放置在零售商店的出口门处的位置信息；

将所述 DHCPDISCOVER 请求发送到动态主机配置协议服务器；

接收来自所述动态主机配置协议服务器的专门针对所述射频识别读取器的供给信息；以及

根据所述供给信息供给所述射频识别读取器，从而使得所述射频识别读取器能够读取经过所述出口门的射频识别标签，并能够将射频识别标签信息发送到射频识别网络。

15. 如权利要求 14 所述的方法，还包括以下步骤：利用所述射频识别标签信息来自动更新由所述零售商店、至少一个产品的制造者和至少一个产品的配发者所维护的数据库。

16. 如权利要求 14 所述的方法，还包括以下步骤：利用所述射频识别标签信息来使金融账户被借记产品的花销。

17. 如权利要求 14 所述的方法，还包括以下步骤：利用所述射频识别标签来更新商业计划。

18. 如权利要求 17 所述的方法，其中，所述商业计划包括营销计划、制造计划、配发计划和销售计划。

19. 一种射频识别网络，包括：

多个射频识别设备；

将所述射频识别设备连接到所述射频识别网络的多个交换机；以及  
动态主机配置协议服务器，其中所述多个射频识别设备中的一个或多个包括：

用于形成 DHCPDISCOVER 请求的装置，所述 DHCPDISCOVER 请求包括射频识别设备的电子产品代码；以及

用于经由交换机将所述 DHCPDISCOVER 请求发送到所述动态主机配

置协议服务器，并用于接收来自所述动态主机配置协议服务器的为所述射频识别设备专门定制的供给信息的装置；其中，所述交换机包括用于将指示所述射频识别设备的位置的位置信息包括在所述 DHCPDISCOVER 请求中的装置；并且其中，所述动态主机配置协议服务器包括：

用于接收 DHCPDISCOVER 请求的装置；以及

用于根据被包括在所述 DHCPDISCOVER 请求中的电子产品代码和介质访问控制地址自动识别射频识别设备，并用于根据被包括在所述 DHCPDISCOVER 请求中的所述位置信息定位所述射频识别设备的装置。

## 定位和供给 RFID 设备的方法和设备及相关网络设备

### 技术领域

本发明涉及供给 (provision) RFID 设备和相关网络设备。

### 背景技术

包含通用产品代码 (“UPC”) 的条形码已经成了现代生活中几乎无所不在的特征。商业流中的绝大多数产品以及包装、容器和其他元素现在都带有条形码, 以允许进行便利的跟踪和库存控制。

但是, 条形码有一些缺点。条形码是“只读”的, 因为它们只是一组打印的不能被更新的机器可读平行条。条形码不能发射信息, 而是必须被扫描器读取。条形码必须在相对较短的距离内被扫描, 并且必须朝向适当的方向, 以便条形码被读取。

为了克服条形码的缺点并且添加更强大的功能, 已经开发出了“智能标签”, 这种“智能标签”一般由 RFID 标签实现。RFID 标签已被用于跟踪物品, 例如航空行李、零售环境中的服装物品、奶牛和公路通行费。如图 1 所示, RFID 标签 100 包括微处理器 105 和天线 110。在该示例中, RFID 标签 100 由 RFID 读取器 125 所生成的磁场 145 提供能量。标签的天线 110 拾取磁信号 145。RFID 标签 100 根据编码在标签中的信息调制信号 145, 并将经调制的信号 155 发射到 RFID 读取器 125。

RFID 标签使用电子产品代码 (“EPC” 或 “ePC”) 格式来对信息编码。EPC 码包括可变长度比特的信息 (常见格式是 64、96 和 128 比特), 其允许了识别个体产品以及相关联的信息。如图 1 所示, EPC 120 包括头部 130、EPC 管理者字段 140、对象类别字段 150 和序列号字段 160。EPC 管理者字段 140 包含制造者信息。对象类别字段 150 包括产品的库存单位 (SKU) 号码。序列号字段 160 是能够唯一地标识个体产品的特定实例的 40 比特字段, 即, 不只是某种样式或型号, 而是具体到一个

样式和型号的特定“序列号”。

理论上，RFID 标签和相关联的 RFID 设备（例如 RFID 读取器和打印机）可形成用于跟踪产品（或产品群组）及其历史的网络的一部分。但是，各种各样的困难妨碍了这一理论的实现。需要 RF 工程师花费大量时间和精力的一问题是开发具有可接受的性能水平的低成本 RFID 标签。感性耦合的 RFID 标签具有可接受的性能水平。这些标签包括微处理器、金属线圈以及玻璃或聚合物封装材料。不幸的是，用于感性耦合的 RFID 标签中的材料使得它们对于广泛使用来说太昂贵：一个无源纽扣标签的成本约为\$1，而用电池供电的读/写型标签的成本可能为\$100 或更多。

容性耦合的 RFID 标签使用导电墨水来取代感性 RFID 标签中使用的金属线圈。墨水被 RFID 打印机打印在纸签上，从而产生成本较低的一次性 RFID 标签。但是，传统的容性耦合 RFID 标签具有非常有限的范围。近年来，RF 工程师已经在努力争取将容性耦合的 RFID 标签的范围扩展到超过约一厘米。

部分由于大量精力被花在解决前述问题上，所以用于联网 RFID 设备的现有技术系统和方法是相当原始的。RFID 设备最近才被部署为带有网络接口。对于现有技术 RFID 设备的设备供给不是自动的，而是需要一个耗时的过程来配置每个设备。现有技术 RFID 设备和系统不适合于 RFID 设备的网络的大规模部署。

并且，传统的 RFID 设备具有少量的可用存储器。典型的 RFID 设备可能具有约 0.5 Mb 的闪存以及总共 1 Mb 的总存储器。RFID 设备的小存储器限制了对这里提到的问题的可能的解决方案的范围。此外，RFID 设备一般使用专用操作系统，例如 RFID 设备中使用的（一个或多个）微处理器的制造者的操作系统。

此外，许多 RFID 设备是在不利的工业环境中（例如仓库或工作）由技术相对不熟练的“IT”人员部署的。例如，如果在一个位置部署的设备例如发生故障，则它可能就只是简单地被移去并被用在另一个位置部署的正常工作的设备所替换。

此外，RFID 设备被部署为具有关于最初部署时设备的被部署位置的

“静态”知识。在实践中，如果另一个设备损坏或不正常工作，则 RFID 设备被移动。通常，希望允许 RFID 设备的移动。但是，如果 RFID 设备被移动，则现有技术系统不知道 RFID 设备被移动到了什么位置。

在一些网络内大量部署设备，其中包括但不限于 RFID 读取器、RFID 打印机、VoIP 电话和用于制造中的设备，已经要成为常事了。这些设备通常具有独特的特性，例如流量类型、带宽要求、安全性需求等等。因此，这种设备要求特定的网络配置，例如，服务质量（“QoS”）、安全性设备、VLAN 或 VSAN 等等，以适当地支持它们的希望的功能。

图 10 示出了网络 1000 的一部分，其中网络设备 1005（在本示例中是 Cisco Systems, Inc 开发的 Catalyst™ 交换机）连接到多个设备，包括 RFID 读取器 1010。在本示例中，RFID 读取器 1010 经由快速以太网连接而连接到端口 1020。对于网络设备 1005 的每个端口，可以配置各种属性，例如 QoS、安全性、端口速度、描述，等等。

在网络 1000 内，可以部署大量设备和相关联的网络设备。一般，对于用户来说，部署设备并管理相关联的基础设施组件，例如交换机和其他网络设备，是一个单调且耗时的过程。例如，配置交换机端口设置的过程目前是手工过程，其中对于一个端口，必须单独选择和使能每个所需的属性。

该手工配置过程目前阻碍着大模型 RFID 网络、制造设备网络等的部署。希望提供克服现有技术的至少一些局限性的改进的方法和设备。

## 发明内容

提供了用于识别和供给网络中的个体 RFID 设备的方法和设备。根据本发明的一些实现方式，EPC 代码信息和现有网络标准的组合形成了识别和供给方法的基础。例如，MAC 地址信息和 EPC 信息可被组合起来以标识特定的设备以及它在网络中的位置。更高级别的应用可被告知例如特定 RFID 设备可供使用。

对于使用动态主机配置协议（“DHCP”）的实现方式，DHCP 选项可被用于传递标识、位置和供给信息。例如，选中的 DHCP 选项可被用于



指示设备是否是 RFID 设备、提供唯一地标识该特定设备的 EPC 码，指示使用该设备的公司名称和指示设备如何被使用。

本发明的一些这样的实现方式利用 DHCPINFORM (RFC 2131) 和 DHCP 选项 (RFC 2132 和 3004) 来传递当前的供给和个性信息。此外，本发明的一些这样的实现方式利用来自 DHCP 服务器的 DHCPFORCERENEW 命令 (RFC 3203) 来根据需要发起更新或完成重配置。

为了保证 DHCPFORCERENEW 命令的安全，一些实现方式提供了被缓存的利用客户端 EPC 被哈希的秘密，其与来自 RFID 设备的 DHCP 请求和来自 DHCP 服务器的响应包括在一起。一些实现方式采用域名服务 (“DNS”) 和动态 DNS (“DDNS”) 来允许容易地识别 RFID 设备。

本发明的一些方面提供了一种用于唯一地供给射频识别 (“RFID”) 设备的方法。该方法包括以下步骤：在网络上接收供给请求；根据包括在供给请求中的电子产品代码 (“EPC”) 和介质访问控制 (“MAC”) 地址自动识别 RFID 设备；以及根据包括在供给请求中的位置信息自动定位 RFID 设备。该方法可由比如动态主机配置协议 (“DHCP”) 服务器这样的网络设备来执行。

该方法可包括以下步骤：将供给请求中的信息与其他信息相比较，以确认 RFID 设备。该方法还可包括以下步骤：确定 RFID 设备先前是否已被引导和/或确定先前是否已为 RFID 设备建立了供给信息。

当确定出先前已为 RFID 设备确立了供给信息时，该 RFID 设备可被供给。如果确定出先前没有为 RFID 设备确立供给信息，则可将该 RFID 设备分类为不受信任的设备。

本发明的另一些方面提供了一种用于唯一地供给 RFID 设备的方法。该方法包括以下步骤：形成包括 RFID 设备的 EPC 和指示 RFID 设备的位置的位置信息的 DHCPDISCOVER 请求；将 DHCPDISCOVER 请求发送到 DHCP 服务器；以及接收来自 DHCP 服务器的专门针对该 RFID 设备的供给信息。

形成步骤可涉及在 DHCPDISCOVER 请求的选项字段 (例如选项 61)

中包括 EPC。形成步骤可涉及包括 DHCPDISCOVER 请求的指示 DHCPDISCOVER 请求来自 RFID 设备的信息（例如在选项 60 中）。形成步骤还可涉及在 DHCPDISCOVER 请求中包括指示提供、拥有或操作 RFID 设备的公司的名称的信息。此外，形成步骤可涉及包括 DHCPDISCOVER 请求的关于形成 DHCPDISCOVER 请求的 RFID 设备的类型的信息（例如在选项 77 中）。

RFID 设备可在形成步骤的第一部分期间包括 EPC。中继代理可在形成步骤的第二部分期间将位置信息包括在 DHCPDISCOVER 请求中。或者，RFID 设备可将位置信息包括在 DHCPDISCOVER 请求中。

本发明的一些实施例提供了一种 RFID 设备，包括：闪存；被配置为根据闪存中的指令，形成在选项 61 中包括 RFID 设备的 EPC 的 DHCPDISCOVER 请求的处理器；以及用于将 DHCPDISCOVER 请求发送到 DHCP 服务器的网络接口。

本发明的其他实施例提供了一种用于唯一地供给 RFID 设备的方法，包括：形成包括 RFID 设备的 EPC 和指示 RFID 设备的位置的位置信息的 DHCPDISCOVER 请求；将 DHCPDISCOVER 请求发送到 DHCP 服务器；以及接收来自 DHCP 服务器的专门针对该 RFID 设备的供给信息。

本发明的其他实施例提供了一种用于唯一地供给 RFID 设备的方法，包括：在网络上接收供给请求；根据包括在供给请求中的 EPC 和 MAC 地址识别 RFID 设备；以及根据包括在供给请求中的位置信息定位 RFID 设备。

本发明的其他方面提供了用于在网络中部署 RFID 设备的方法。一种这样的方法包括以下步骤：形成包括 RFID 读取器的 EPC 和指示 RFID 读取器被放置在零售商店的出口门处的位置信息的 DHCPDISCOVER 请求；将 DHCPDISCOVER 请求发送到 DHCP 服务器；接收来自 DHCP 服务器的专门针对该 RFID 读取器的供给信息；以及根据供给信息来供给 RFID 读取器，从而使得 RFID 读取器能够读取经过出口门的 RFID 标签并将 RFID 标签信息传送到 RFID 网络。RFID 标签信息可包括产品信息和/或购物者

信息。

该方法可包括以下步骤：利用 RFID 标签信息来使金融账户被借记了产品的花销。RFID 标签信息可被用于自动更新由零售商店维护的数据库和/或由至少一个产品的制造者/生产者、批发者和/或配发者所维护的数据库。RFID 标签可被用于更新商业计划，例如营销、制造、配发和销售计划。

本发明的其他实施例提供了一种 RFID 网络，包括：多个 RFID 设备；将 RFID 设备连接到 RFID 网络的多个交换机；以及 DHCP 服务器。在一些这样的实施例中，所述多个 RFID 设备中的至少一些被配置为执行以下操作：形成包括 RFID 设备的 EPC 的 DHCPDISCOVER 请求；经由交换机将 DHCPDISCOVER 请求发送到 DHCP 服务器；以及接收来自 DHCP 服务器的为 RFID 设备专门定制的供给信息。交换机被配置为将指示 RFID 设备的位置的位置信息添加到 DHCPDISCOVER 请求。DHCP 服务器被配置为接收 DHCPDISCOVER 请求，根据包括在 DHCPDISCOVER 请求中的 EPC 和 MAC 地址自动识别 RFID 设备，并且根据包括在 DHCPDISCOVER 请求中的位置信息自动定位 RFID 设备。

还提供了用于识别终端设备并自动配置相关联的网络设置的方法和设备。本发明的优选实现方式不要求用户手工识别连接类型（例如 RFID、IP 电话、制造设备等）或手工配置网络设备。因此，这样的实现方式允许了自动的交换机配置，即使对于使用不一致的协议和/或非公知协议的设备也是如此。

本发明的一些方法采用了与流量探听相结合的 DHCP 选项，以识别设备并自动应用适当的交换机端口配置。本发明的一些这样的实现方式触发 Cisco Systems 的 SmartPorts™ 软件来配置网络设备的端口。SmartPorts 软件的一些方面在 2004 年 7 月 21 日递交的美国专利申请 No. 10/896,410 中描述，这里通过引用将其并入。但是，本发明并不局限于经由 SmartPorts™ 的实现方式；任何便利的用于网络设备端口的自动配置的软件都可根据本发明而使用。

本发明的一些实现方式提供了一种用于确立网络设备端口设置的方

法，该方法包括以下步骤：接收来自设备的 DHCPDISCOVER 请求，以及基于 DHCPDISCOVER 请求中的信息，确定是否有适当的宏可用于配置最初在其上接收 DHCPDISCOVER 请求的网络设备的端口。

该方法还可包括当确定出有适当的宏可用时，应用该适当的宏。该方法优选地包括以下步骤：确定是否已以适合于该设备的方式配置了端口。

确定步骤可包括确定设备个性，识别设备和/或检查至少一个 DHCP 选项或 DHCPDISCOVER 请求的其他成分。“其他成分”例如可以是 DHCP 消息头部的一个或多个部分。确定步骤可由最初在其上接收 DHCPDISCOVER 请求的网络设备执行，也可不由最初在其上接收 DHCPDISCOVER 请求的网络设备执行。例如，DHCPDISCOVER 请求最初可被交换机端口所接收，并且确定步骤可由 DHCP 服务器、边缘服务管理服务器、认证服务器和专用于端口配置的设备之一执行。

本发明的一些实施例提供了至少一种用于确立网络设备端口设置的方法。这些实施例包括用于接收来自设备的 DHCPDISCOVER 请求的端口，以及被配置用于基于 DHCPDISCOVER 请求中的信息确定是否有适当的宏可用于配置该端口的至少一个逻辑设备。

逻辑设备可检查 DHCPDISCOVER 请求的一个或多个 DHCP 选项。端口和（一个或多个）逻辑设备可被包括在单个设备内，或者可被置于分离的设备中。例如，端口和（一个或多个）逻辑设备可被包括在单个交换机或 DHCP 服务器内。

本发明的其他实施例提供了一种网络设备，其包括这些部件：多个端口；存储设备；以及被配置为经由第一端口接收来自设备的 DHCPDISCOVER 请求并利用用于设备的适当配置参数配置第一端口的至少一个逻辑设备。

逻辑设备还可被配置为将 DHCPDISCOVER 请求的拷贝转发到第二设备。逻辑设置可根据接收自第二设备的指令配置第一端口。第二设备例如可以是 DHCP 服务器、边缘服务管理服务器、认证服务器和专用于端口配置的设备。

本发明的方法至少可部分地由硬件和/或软件实现。例如，本发明的一

些实施例提供了包含在机器可读介质中的计算机程序。计算机程序包括用于控制一个或多个设备执行这里描述的方法的指令。

### 附图说明

图 1 是示出了一个 RFID 标签的图。

图 2 示出了根据本发明的示例性 RFID 网络。

图 3 是可被配置为执行本发明的一些方法的示例性 RFID 读取器的框图。

图 4 是可被配置为执行本发明的一些方法的示例性 RFID 打印机的框图。

图 5 是可被配置为执行本发明的一些方法的示例性 RFID 系统的框图。

图 6 是提供对本发明的一些方法的概览的流程图。

图 7 是提供对本发明的另外的方法的概览的流程图。

图 8 是提供对本发明的一些实现方式的概览的流程图。

图 9 示出了可被配置为实现本发明的一些方法的网络设备的示例。

图 10 是示出了交换机和附接的 RFID 设备的网络图。

图 11A 示出了例性 SmartPorts™ 宏。

图 11B 示出了用于根据 SmartPorts™ 宏配置端口的示例性命令集。

图 12A 是提供对本发明的一种方法的概览的流程图。

图 12B 是示出了图 12A 所示的方法的实现方式的网络图。

图 13 是提供对本发明的另一种方法的概览的流程图。

图 14 是示出了用于实现本发明的一些方面的网络设备的框图。

### 具体实施方式

在本申请中，阐述了许多具体细节以提供对本发明的充分理解。但是，对于本领域的技术人员来说显而易见的是，没有这些具体细节中的一些或全部也能实现本发明。在其他情况下，没有详细描述公知的过程步骤，以免使本发明模糊。

虽然本发明包括用于识别和供给网络中的个体 RFID 设备的方法和设备，但是本发明的许多方面也可以应用于识别和供给网络中的其他类型的设备。类似地，虽然这里的许多论述适用于使用 DHCP 协议的实现方式，但本发明并不是特定于协议的，而是例如可以用于使用 UPnP、802.1ab 或类似的发现协议的实现方式中。同样，虽然这里描述的实现方式谈到了示例性的 DHCP 选项，但是其他 DHCP 选项也可被有利地用于实现本发明。

RFID 设备执行不同的功能，并且可以按依赖于其位置的不同方式与上游系统接口。它们所执行的功能，以及用于执行这些功能的唯一的设置，在这里将被称为设备的“个性 (personality)”。这里所使用的“供给 (provision)”一个设备可包括但不限于提供网络配置、提供个性配置、将设备结合到网络数据库中，以及使设备能够具有软件（例如商业过程软件）。

本发明的方法和设备具有非常广泛的实用性，不论是公共领域还是私有领域。任何企业都需要跟踪其设备如何被部署，不论该设备是用于商业目的还是军事目的，等等。根据本发明而联网的 RFID 设备可提供用于允许企业跟踪设备和产品（或产品群组）的必要信息。将由根据本发明而联网的 RFID 设备提供的信息对于包括制造、配发、销售和营销规划在内的企业资源规划将会有很大益处。

利用本发明的设备和方法，RFID 标签和相关联的 RFID 设备（例如 RFID 读取器和打印机）可形成用于跟踪产品及其历史的网络的一部分。例如，希望购买带有 RFID 标签的产品的购物者可以不用在结账队列中等待购买选中的产品，而是例如可以将产品运送通过附近的具有 RFID 读取器的门。关于产品的 EPC 信息可被读取器提供给 RFID 网络，并可被用于自动更新商店库存，使金融账户被借记，更新制造者的、配发者的和零售者的产品销售数据库，等等。

读/写型 RFID 标签可捕捉关于产品或产品群组的信息，例如作用在产品上的温度和其他环境变化、应力、加速度和/或振动。对于较易变质或遭其他损坏的产品，例如易腐烂的食品和易碎物品，记录这种信息尤其有用。通过利用本发明的方法，该信息将被用于更新由各种实体（例如制造

者、批发者、零售者、运输公司和金融机构)所维护的数据库。该信息不仅将被用于解决争议(例如关于产品损坏的责任),还可用于提高顾客满意度,避免健康危险等等。

本发明的一些方面使用 EPC 码信息和现有联网标准的修改版本的组合,来识别、定位和供给位于网络中的 RFID 设备,例如 RFID 读取器和 RFID 打印机。这种网络的一个示例在图 2 中示出。这里,RFID 网络 200 包括仓库 201、工厂 205、零售店 210、金融机构 215 和总部 220。本领域的技术人员将会意识到,网络 200 可包括许多其他元素和/或图 2 所示的部件的多个实例。例如,网络 200 可包括多个仓库、工厂,等等。

在该图中,产品 227 正被卡车 275 递送到仓库 201。已经含有 RFID 标签的产品 227 被递送经过门 225。在本示例中,RFID 读取器 252 连接到交换机 260 的端口 262。这里,交换机 230 和 260 经由网关 250 和网络 225 连接到 RFID 网络 200 的其余部分。网络 225 可以是任何便利的网络,而在本示例中,网络 225 是因特网。RFID 读取器 252 读取经过门 225 的每个产品,并在 RFID 网络 200 上传送与每个产品相对应的 EPC 码。

RFID 标签可用于不同级别的产品配发系统。例如,可以有用于一货盘的箱子的 RFID 标签、用于货盘中的每个箱子的 RFID 标签,以及用于每个产品的 RFID 标签。因此,在产品 227 进入仓库 201 之后,它们被聚集到箱子 246 中。RFID 打印机 256 为每个箱子 246 制作一个 RFID 标签。在本示例中,RFID 打印机 256 连接到交换机 260 的端口 266。RFID 打印机 256 可在仓库 201 中的 PC 247、总部 220 中的 PC 267 之一或某个其他设备的控制之下工作。

连接到端口 214 的 RFID 读取器 224 读取输送带 244 上的每个箱子 246 和产品 227 的 EPC 码,并在网络 200 上传送该信息。类似地,连接到端口 216 的 RFID 读取器 226 读取从门 204 出去的每个箱子 246 和产品 227 的 EPC 码,并在网络 200 上传送该信息。箱子 246 被装载到卡车 285 上,以便配发到产品链的另一部分,例如到零售店 210。

网络 200 中的每个 RFID 设备优选地具有适合其预期用途的“个性”。例如,如果经授权的人或物体进入门 225,则设备 252 可以促使发

出使放心的音调和/或使绿灯闪烁。但是，如果产品从门 225 出去或未经授权的人进入门 225 或从门 225 出去，则设备 252 可能促使响起警报和/或将警告发送到网络 200 上的管理员。

图 3 示出了可被配置为执行本发明的方法的 RFID 读取器。RFID 读取器 300 包括一个或多个 RF 无线电装置 305，用于将 RF 波发射到 RFID 标签，并接收来自 RFID 标签的经调制的 RF 波。RF 无线电装置 305 提供被模数转换器（未示出）转换并被输送到 RFID 读取器 300 的其他部件的原始 RF 数据。在一些实施例中，这些数据在经由网络接口 325 被传送到网络 200 的其他部分之前，至少暂时地被 CPU 310 存储在存储器 315 中。网络接口 325 可以是任何便利类型的接口，例如以太网接口。

闪存 320 被用于存储用于引导/初始化 RFID 读取器 300 的程序（“引导加载程序”）。引导加载程序通常被存储在闪存 320 的单独的分区区域中，它还允许了 RFID 读取器 300 在掉电时恢复，等等。在本发明的一些实施例中，闪存 320 包括用于控制 CPU 310 以形成下文参考图 6 描述的“DHCPDISCOVER”请求的指令，以发起供给/配置周期。在一些实现方式中，闪存 320 被用于存储例如在这样的周期期间从 DHCP 服务器获得的个性信息和其他配置信息。

但是，在优选实现方式中，这种信息在被从例如 DHCP 服务器接收到之后，仅被存储在易失性存储器 415 中。保持 RFID 设备“哑（dumb）”是有一些优点的。例如，哑 RFID 设备的网络允许许多处理负荷被集中起来（例如由网络 200 的服务器 270 执行），而不是由 RFID 设备执行。或者，处理负荷可被分散，但只被分散到受信任的设备（例如网络 200 的 PC 247）。

配置信息例如被从中央服务器下载到存储器 315。更新可由中央服务器或选中的受信任设备发动。新版本的映像文件（例如操作 RFID 设备所必需的运行的基本映像）被拷贝到闪存 320 中。RFID 设备的另一些实施例实现了本发明的方法，但没有闪存。

更新型的 RFID 设备还包括干接触式输入/输出导线，以连接到信号灯、工业网络或等同物。这些更新型的 RFID 设备一般在存储量、闪存、



CPU 能力和确定其视野内的 RFID 标签的数目、类型和内容的方法方面已经有所发展。

图 4 是示出可被配置为执行本发明的一些方法的示例性 RFID 打印机 400 的框图。RFID 打印机 400 具有许多与 RFID 读取器 300 相同的组件，并且可以按与 RFID 读取器 300 相同的一般方式来配置。

RFID 打印机还包括打印机接口 430，该接口可以是标准的打印机接口。打印机接口例如根据经由网络接口 425 从网络 200 接收的指令，为每个 RFID 标签打印一个标记。

RF 无线电装置 405 是传出无线电装置，用于在 CPU 410 的控制下向 RFID 标签的天线发送 RF 信号，从而对标签的微处理器上的信息（例如 EPC）编码。优选地，RF 无线电装置 405 随后检查经编码信息的正确性。RFID 标签被夹由在打印机接口 430 产生的标记内。

图 5 示出了包括控制部分 501 和 RF 无线电部分 502 的 RFID 系统 500。控制部分 501 的组件与以上参考图 3 和图 4 描述的那些基本类似。控制部分 501 的互连装置 530 被配置用于与 RF 无线电部分 502 的互连装置 535 通信。通信可以经由任何便利的介质和格式，例如无线、串行、点到点串行等等。虽然图 5 中只示出了一个 RF 无线电部分 502，但是每个控制部分 501 可控制多个 RF 无线电部分 502。RFID 系统 500 可被部署在单个机架或机箱上（例如叉车上）或者多个机箱中。

DHCP 协议被用于本发明的一些优选实现方式中，这是因为它提供了多种便利的特征。例如，DHCP 协议允许定义 TCP/IP 地址的池或“范围”。DHCP 服务器可将这些 TCP/IP 地址临时分配或“租借”给主机设备。在租借期间未被使用的 IP 地址被返回到未分配的 IP 地址的池。此外，DHCP 服务器将会提供 TCP/IP 适当工作所需的所有相关配置设置，例如默认路由器、域名服务（“DNS”）服务器、子网掩码等。

对于使用 DHCP 协议的实现方式，DHCP 选项可被用于传递供给信息。DHCP 协议在 RFC 2131 中定义，DHCP 选项例如在 RFC 2132、3004 和 3046 中被阐述。这里通过引用并入 RFC 2131、2132、3004 和 3046，用于所有目的。

在一些优选实现方式中，与 RFID 设备相对应的 EPC 被置于从 RFID 设备发送到 DHCP 服务器的 DHCP 请求内。EPC 唯一地标识 RFID 设备。一些实现方式采用了域名服务（“DNS”）和动态 DNS（“DDNS”），以允许更容易地识别 RFID 设备。

现将参考图 6 描述对本发明的一些这样的实现方式的概览。向 DHCP 服务器发出对 IP 地址的起动的设备通过包括“DHCPDISCOVER”请求的分组来完成这一点。该命令包括设备的介质访问控制（“MAC”）地址。根据一些优选实现方式，RFID 设备（例如 RFID 读取器 300 的 CPU 310）形成“DHCPDISCOVER”请求分组，其包括各种 DHCP 选项字段中的信息（步骤 601）。RFID 设备利用指示该设备是 RFID 设备的代码，对 DHCP “类别标识符”选项 60 编码。换言之，“RFID”将会是编码在选项 60 中的新类型的“类别”。

在本示例中，RFID 设备将其自身的 EPC 编码在为选项 61 预留的字段中。RFID 设备还将公司名称（例如提供、拥有或正在使用 RFID 设备的公司的名称）编码在 DHCP 选项 43 中。

根据本发明的不同实现方式，可以按各种方式来使用选项 77。在一些实现方式中，选项 77 将被用于指示 RFID 设备的类型，例如 RFID 设备是 RFID 读取器或 RFID 打印机。在一些实现方式中，选项 77 还可包括关于 RFID 设备的功能或“个性”的信息。例如，选项 77 可指示 RFID 设备是传入 RFID 读取器、传出 RFID 读取器、装配线上或零售商店中的 RFID 读取器或打印机，等等。

再次参考图 2，如果请求是来自 RFID 设备 252 的，则该设备将把指示该设备是 RFID 读取器的信息编码在选项 77 中。在一些实现方式中，选项 77 还指示 RFID 设备 252 具有适合于被放置在入口门处的个性。一些实现方式包括关于设备 252 的当前个性的更详细信息。例如，选项 77 可指示除了读取 EPC 码并将它们上载到 RFID 网络之外，设备 252 还将使得如果经授权的人或物体进入门 225，则绿灯闪烁，而如果产品从门 225 出去，则红灯闪烁、响起警报以及将警告发送到网络上的管理员。该信息例如可以根据与入口门处的 RFID 读取器的一系列合适个性之一相对应的数

字来编码。

希望为网络中的 RFID 设备确定和提供位置信息。具有以太网或交换机端口的交换机和无线网桥被认为是静态的，并具有指定的名称和位置。根据本发明的一些实现方式，位置信息例如被 RFID 设备所附接到的网络设备，添加到 RFID 设备的 DHCPDISCOVER 请求中（步骤 610）。

一些这样的实现方式以新的方式使用 DHCP 选项 82（RFC 3046），以确定 RFID 设备所连接到的交换机端口和交换机。例如，交换机可将以下两个信息元素插入到来自附接的 RFID 设备的任何 DHCP 请求中：选项 82，子选项 1：代理电路 ID（Agent Circuit ID）；以及选项 82，子选项 2：代理远程 ID（Agent Remote ID）。代理电路 ID 是交换机的名称或标识符。代理远程 ID 是交换机端口的名称或标识符。

例如，如果请求是来自图 2 的 RFID 设备 226 的，则网络设备 230 在步骤 610 中将位置信息添加到请求中。这里，位置信息将被编码在选项 82 中，并将包括标识 RFID 读取器 226 所附接到的网络设备 230 和端口 216 的信息。

在其中 RFID 设备能够确定其自身的位置（例如从 GPS 坐标确定）的另一些实施例中，RFID 设备可将位置信息编码在 DHCPDISCOVER 请求或其他命令中。

可以有多个服务同一网络的 DHCP 服务器。服务器如何作出响应例如可以依赖于每个服务器是否忙、它是否已经分发了它所有的地址，等等。随着 RFID 试验网络（pilot network）的出现和发展，它们将与包括采用 DHCP 协议的网络在内的现有网络交织在一起。供给 RFID 设备的 DHCP 服务器（例如图 2 的服务器 270）将会对例如编码在选项 60 中的将设备的类别标识为“RFID”的“DHCPDISCOVER”命令作出响应。本领域的技术人员将会意识到，其他选项也可用于这个目的。相反，不供给 RFID 设备的 DHCP 服务器将不对将设备类别标识为“RFID”的“DHCPDISCOVER”命令作出响应。此外，如果非 RFID DHCP 服务器作出了响应，则 RFID 设备将能够从它所接收到的 DHCP 选项响应中确定出不完整的 DHCP 响应，并丢弃它，并且将会优选来自 RFID DHCP 服务器

的响应。因此，本发明的方法允许了将 RFID 网络集成到 DHCP 协议的现有框架内。

在步骤 615 中，DHCP 服务器确定在关于已知 RFID 设备、它们的预期功能和配置等的信息的数据库内是否有关于发出请求的设备的信息。例如，DHCP 服务器可检查编码在请求中的 EPC，并确定在数据库中是否有用于具有相应 EPC 的设备的信息。

如果有，则在步骤 620 中，服务器将 DHCP 请求中的信息与存储的关于 RFID 设备的信息相比较。该信息可能处于例如由负责 RFID 网络的 IT 人员更新的数据库中（例如存储在存储设备 265 之一中）。例如，MAC 地址信息和 EPC 信息可被组合，以标识特定设备及其在网络中的位置。更高级别的应用可被告知例如特定 RFID 网络可供使用。

通过检查接收到的数据，服务器于是可以确定 RFID 设备的类型、身份、位置和个性（如果有的话）。通过将接收到的数据与数据库中的信息相比较，服务器于是可以确定例如这个 RFID 设备是否已经移动以及现在它处于什么位置。在优选实现方式中，DHCP 服务器可以确定 RFID 设备的当前个性（例如通过检查选项 77 数据），并可以将当前个性与所期望的个性相比较。

在步骤 625 中，DHCP 服务器向 RFID 设备提供数据库中指示的配置信息等。例如，DHCP 服务器可指示 RFID 设备的时间服务器、SYSLOG 服务器、设备的配置文件的位置、映像文件，等等。如果 RFID 设备的当前个性不匹配期望个性（或者如果请求未指示当前个性），则根据一些实现方式，DHCP 服务器可向设备提供用于使能期望个性的信息（例如计算机程序、配置设置等等）。

例如，假定 EPC 码指示设备是 RFID 读取器 252，并且选项 77 指示 RFID 设备 252 具有适合被放置在入口门处的个性。但是，请求中的位置信息可能指示发出请求的设备已经被移动并且现在位于出口门处。或者，数据库可能指示设备被放置在了过去被用作入口门但现在将被用作出口门的门处。这可能是制造设施或仓库处的周期性（例如每小时、每日、每周或每月）的变化，或者可能由设施的重配置引起。

因此，RFID 设备 252 的期望个性现在是适合于出口门的个性。但是，可能存在例如依赖于作出请求的设备的能力、出口门的预期用途等而可提供给设备 252 的一系列不同的“出口门”个性。例如，具有较少的能力（例如较小的存储器）的设备可能被赋予相对较简单的出口门功能。例如，这种设备可被赋予例如在特定类型的产品从门出去时使绿灯闪烁，并在其他物品从门出去的情况下向 IT 人员传送通知消息和/或促使响起警报的能力。

但是，具有较大能力的设备可被赋予相对较复杂的出口门功能。例如，设备可被赋予如果特定类型的产品在预期时间出去、如果从门出去的产品数目处于预定范围内等，则使绿灯闪烁的能力。

重新指定设备个性的这种灵活性允许了 RFID 网络基于位置、时段或任何其他合适的标准，使相同设备类型具有多个个性。此外，这种灵活性允许了设备的移动或重定位（不论这种移动是否已被预先批准），然后使得设备能够被自动地“重个性化”而适合于新位置。此外，它允许了基于每设备、每地点的专门功能。

但是，在一些情况下，在数据库中可能没有关于该设备的信息。例如，设备可能是刚刚第一次在 RFID 网络中激活的新 RFID 设备（步骤 630）。在本示例中，设备被置于针对不是受信任的设备的那些设备的“有壁园（walled garden）”中。步骤 630 可包括经由 DHCP OFFER 命令为设备指定预定长度的时间内的不可路由 IP 地址。根据一些实现方式，当数据库中有关于与请求中的信息不一致的关于设备的信息时，DHCP 服务器执行步骤 630。

优选地，步骤 630 包括向更高层应用通知设备已作出请求。以这种方式，负责 RFID 设备所处地点的 IT 人员将被告知：RFID 设备离开了并作出了请求。

根据一些实现方式，步骤 630 包括将 DHCP T1 定时器设置为短间隔，例如 60 秒。在本示例中，RFID 设备将持续地每 60 秒向服务器发送 DHCP 请求，并且服务器将会向设备发送“ACK”，直到以下两个事件之一发生：（1）服务器已被更新（例如被负责 RFID 设备所处地点的 IT 人

员更新)；或者(2)服务器和RFID设备之间的连接断开(步骤635)。

如果服务器在预定时间内被更新，则表明IT人员已确定作出请求的RFID设备是受信任的设备。因此，方法进行到步骤625。如果否，则设备仍被归类为不受信任的设备(步骤630)。优选地，设备的状态仍可例如根据IT人员随后的输入而被改为受信任的(因此是被供给的)设备的状态。

在初始供给配置周期(例如如上所述的)之后，RFID设备可能需要被重新供给，或者它们的个性要被改变。如上所述，希望RFID设备依赖于特定时刻时RFID设备的期望功能而具有唯一的供给和个性。期望功能可根据RFID设备的位置和能力来确定。一些设备可能在相对较长的时间(例如若干月或若干年)中被提供以相同的个性。但是，可能希望在相对较短的时间中，例如在DHCP T1定时器期满之前，改变RFID设备的个性和/或供给信息。大多数当前部署的RFID终端设备不支持RFC 3203(DHCP重配置扩展)。

本发明包括多种用于实现这些目标的方法。现将参考图7描述一种这样的方法。方法700开始于确定是否向网络设备发送关于RFID设备的当前个性的信息(步骤701)。这里，如果已经过一段预定的时间，则RFID设备将向DHCP服务器发送该信息。在本示例中，预定的时间段是一个小时的时间，但它也可以是任何便利的时间段。

如果到了另一个DHCPREQUEST或DHCPINFORM请求应当被发送到DHCP服务器的时间，则RFID设备形成该请求(步骤705)。如果否，则当前个性被维持(步骤702)。在本示例中，信息将会结合被设置为RFID设备的EPC(或等同物)的DHCP选项61和被设置为RFID设备的当前个性的选项77而在DHCP请求(RFC 2131)中被发送。利用DHCPINFORM和DHCP选项，RFID设备能够传递当前标识、供给和个性信息。

在本示例中，被缓存的秘密(例如，利用DHCP消息的内容(包括客户端EPC)而被哈希(hash)的秘密)将被与DHCP请求包括在一起，以便保证响应的安全。该秘密例如可在较早的供给阶段期间被提供，例如在

RFID 设备的初始供给阶段期间被提供。该秘密可被用于 DHCPINFORM 确认过程和其他过程中。

在步骤 710 中，请求被发送。优选地，中继代理利用位置信息更新请求，如上所述（步骤 715）。

在步骤 720 中，服务器将请求中的信息与存储的信息（例如存储在查找表或数据库中的信息）相比较，以确定是否需要更新 RFID 设备进行更新或完全重配置。如果否，则过程返回到步骤 701。如果是，则服务器向 RFID 设备提供必要的更新和/或重配置信息（步骤 725）。

RFID 设备触发前述示例中的更新和/或重配置确定。但是，在其他实现方式中，另一设备（例如 DHCP 服务器）和/或人发起该确定。例如，DHCP 服务器可发起将期望 RFID 设备个性与最后已知的 RFID 设备个性相比较的周期性的过程。或者，IT 工作者可发送指示期望的个性变化的信息（例如向 DHCP 服务器、RFID 设备或另一设备发送）。

根据本发明的一些实现方式，DHCP 服务器利用如 RFC 3203（这里通过引用并入其全文）所定义的 DHCPFORCERENEW 命令来引起更新或完全重配置。RFID 设备的 CPU 注册 ForceRenew 命令，并开始新的供给周期，例如上面参考图 6 所描述的。

为了保证命令的安全，在本示例中，缓存的秘密被哈希在命令内。例如，秘密可被与 RFID 设备的 EPC 码包括在一起。

一种用于创建认证密钥的方法如下：

MD-5 (EPC, Challenge, Secret)

通过添加随机 Challenge（挑战）的变量，哈希代码的重放攻击不能被使用。由于包括了 EPC，可以进一步确证认证来自特定设备。

前述方法允许了按时段而不是简单地按设备“类型”、“类别”或“位置”来唯一确定和供给 RFID 设备。此外，前述方法允许了对终端设备的角色的进行中的验证/核查。此外，这些方法允许了操作管理者让企业资源规划系统控制终端设备，以允许更多功能。

图 8 是示出本发明的示例性商业应用的流程图。本领域的技术人员将会意识到，以下参考图 8 描述的示例只是本发明的许多应用之一。

在步骤 805 中，RFID 设备已根据先前描述的方法之一被供给。RFID 设备的状况与方法 600（在图 6 中示出并在上文描述）中的步骤 640 处的设备的状况相当。在本示例中，RFID 设备是被放置在零售商店的出口门附近的 RFID 读取器。因此，在前述步骤中，设备已被供给以适合于其角色的个性。

在步骤 810 中，购物者带着若干选中的产品从门出去。在步骤 815 中，RFID 读取器读取每个产品的 RFID 标签，并提取 EPC 码和相关产品信息（例如每个产品的价格）。

RFID 读取器还读取标识购物者和购物者为了购买产品而应当被借记的（一个或多个）优选账户的 RFID 标签。例如，购物者可能拥有嵌入在卡、钥匙链或任何其他其中编码有该信息的便利的地方中的 RFID 标签。账户可以是由一个或多个金融机构维护的各种类型的账户。例如，账户可以是支票账户、储蓄账户、信用额、信用卡账户等等中的一种或多种。来自购物者的生物测定数据（例如语音、指纹、视网膜扫描等）也可被获得，并被与存储的生物测定数据相比较，以便验证购物者的身份。

在步骤 820 中，RFID 读取器在 RFID 网络上传送产品信息，其中包括 EPC 码。在本示例中，信息首先被发送到由购物者的 RFID 标签指示的金融机构。

在步骤 825 中，维护购物者的选定账户的金融机构确定是否有足够的资金（或是否有充足的信用）供购物者购买选中的产品。如果有，则购物者的账户被借记，并且交易完成（步骤 830）。

在本示例中，购物者可以选择指明一个或多个备选账户。因此，如果第一账户没有足够的资金或信用，则确定（例如由 RFID 网络上的服务器确定）购物者是否已指示了任何备选账户用于进行购买（步骤 835）。如果是，则在步骤 825 中下一个账户被评估。如果在步骤 835 中确定购物者没有指明额外的账户，则在本示例中，发生某种形式的人为干预。例如，零售商店的出纳员可帮助购物者以便利的方式进行购买。

如果产品中的一些或全部被购买，则关于购买的产品的信息（包括 EPC 码）在 RFID 网络上被传送。例如，该信息优选地被转发到 RFID 网



络上的一个或多个设备（步骤 840），所述一个或多个设备被配置为更新由零售商店或所购买产品的制造者/生产者、配发者、批发者等所维护的一个或多个数据库。在一些实现方式中，关于购物者的信息也在 RFID 网络上传送（例如，如果购物者已授权公开这种信息）。该产品信息（以及购物者信息（可选））可被用于各种目的，例如用于各种类型的商业计划的形成（例如重新进货、营销、销售、配发和制造/生产计划）。

图 9 示出了可被配置为实现本发明的一些方法的网络设备的示例。网络设备 960 包括主中央处理单元（CPU）962、接口 968 和总线 967（例如 PCI 总线）。接口 968 一般包括适合于与适当的介质通信的端口 969。在一些实施例中，接口 968 中的一个或多个包括至少一个独立处理器 974，并且在一些情况下，包括易失性 RAM。独立处理器 974 例如可以是 ASIC 或任何其他适当的处理器。根据一些这样的实施例，这些独立处理器 974 执行这里描述的逻辑的至少一些功能。在一些实施例中，接口 968 中的一个或多个控制比如介质控制和管理这样的通信密集型任务。通过为通信密集型任务提供单独的处理器，接口 968 允许了主微处理器 962 高效地执行诸如路由选择计算、网络诊断、安全性功能等其他功能。

接口 968 一般是以接口卡（有时称为“线路卡”）的形式提供的。接口 968 一般控制网络上的数据分组的发送和接收，并且有时支持与网络设备 960 一起使用的其他外围设备。可以提供的接口包括光纤信道（“FC”）接口、以太网接口、帧中继接口、线缆接口、DSL 接口、令牌环接口等等。此外，可提供各种超高速接口，例如快速以太网接口、吉比特以太网接口、ATM 接口、HSSI 接口、POS 接口、FDDI 接口、ASI 接口、DHEI 接口等等。

当在适当的软件或固件的控制下动作时，在本发明的一些实现方式中，CPU 962 可负责实现与所期望的网络设备的功能相关联的特定功能。根据一些实施例，CPU 962 在软件的控制下完成所有这些功能，所述软件包括操作系统（例如 Linux、VxWorks 等）和任何适当的应用软件。

CPU 962 可包括一个或多个处理器 963，例如来自 Motorola 微处理器系列或 MIPS 微处理器系列的处理器。在另一实施例中，处理器 963 是专

门设计的用于控制网络设备 960 的操作的硬件。在特定实施例中，存储器 961（例如非易失性 RAM 和/或 ROM）也形成 CPU 962 的一部分。但是，存储器可以以许多种方式耦合到系统。存储器块 961 可用于各种目的，例如缓存和/或存储数据、编程指令等等。

不论网络设备的配置如何，它都可采用一个或多个存储器或存储器模块（例如存储器块 965），其被配置为存储数据、用于通用网络操作的程序指令和/或与这里描述的技术的功能相关的其他信息。程序指令例如可控制操作系统和/或一个或多个应用的操作。

由于这种信息和程序指令可被用来实现这里描述的系统/方法，因此本发明涉及包括用于执行这里描述的各种操作的程序指令、状态信息等的机器可读介质。机器可读介质的示例包括但不限于磁介质，例如硬盘、软盘和磁带；光介质，例如 CD-ROM 盘；磁光介质；以及专门配置为存储和执行程序指令的硬件设备，例如只读存储器设备（ROM）和随机访问存储器（RAM）。本发明还可实现在经由诸如空气波、光线路、电线路等适当的介质传播的载波中。程序指令的示例既包括机器代码，例如由编译器产生的机器代码，也包括包含可由计算机利用解释器执行的更高级的代码的文件。

虽然图 9 所示的系统示出了本发明的一个特定网络设备，但是它绝不是可在其上实现本发明的仅有的网络设备体系结构。例如，经常使用具有处理通信以及路由选择计算等的单个处理器的体系结构。此外，其他类型的接口和介质也可与网络设备一起使用。接口/线路卡之间的通信路径可以是基于总线的（如图 9 所示），也可以是基于交换结构（switch fabric）的（例如纵横交换机（cross-bar））。

本发明的一些示例性实现方式涉及使用 SmartPorts™ “宏（macro）” 功能来配置网络设备的端口。但是，也可使用其他这样的工具。在本发明的其他实现方式中，命令行接口（“CLI”）或诸如简单网络管理协议（“SNMP”）或 Netconf® 这样的另一程序接口被用于此目的。

SmartPorts™ 宏的现有实现方式要求用户手工识别连接类型（例如 RFID、制造、IP 电话），然后根据所识别的连接类型配置网络设备。这里

使用的术语“宏”有时将被用来表示两重含意：用于配置例如网络设备的产品的命令，以及从这种宏的应用而得到的配置。可利用例如命令行接口或比如 CMS 这样的网络管理工具来每端口地配置网络设备。

现将参考图 11A 描述用于配置 RFID 设备的端口的示例性 Cisco SmartPorts™ 宏。行 1101 被用于建立宏的名称，在本例中是 RFID\_Macro1。使用易于被识别为是用于 RFID 设备的一种类型的宏的名称，以允许可以对多个设备类型有多个宏以及对 RFID 设备有多个宏，这将会是有帮助的。

行 1103 将使 RFID VLAN 被指定，并且线路 1105 将交换机端口置于“访问”模式。行 1107 指定一个通用描述给接口，该描述指示其用途，在本示例中是到 RFID 设备的连接。行 1109 赋予端口安全性，并将端口限制到单个介质访问控制（“MAC”）地址。

根据行 1111，当超过最大数目的 MAC 地址时，丢弃来自额外的源 MAC 地址的流量。此外，生成 SNMP 陷阱和系统日志（syslog）消息。行 1113 使安全 MAC 地址在 10 分钟不活动之后过期。

行 1115 将端口配置为不需要根据生成树协议（spanning tree protocol）动作的边缘设备端口。因此，桥端口数据单元（“BPDU”）分组不会被允许从此端口进入网络。“生成树端口快速（Spanning-tree portfast）”允许端口迅速进入转发状态。

行 1117 将广播和多播风暴控制限度设置为接口带宽的 20%。正如本示例中的其他设置那样，此限度应当基于要与端口通信的设备的预期要求。行 1119 将从设备传入的 DHCP 分组速率限制应用到每秒 100 个分组。

行 1121 是设备的 QoS 的一个示例。例如如果该设备是发送被标记了 DSCP 的分组的 RFID 读取器，并且如果这些值应当被信任，则该 QoS 是适用的。

图 11B 给出了如何将前述 SmartPorts 宏应用到交换机端口的一个示例。图 11B 是用于配置端口的 CLI 会话的拷屏图。行 1151 识别要被配置的交换机（“DC\_Switch1”）。行 1155 是来自交换机 DC\_Switch1 的提

示。行 1160 将接口配置为快速以太网接口。

行 1165 将选中的宏应用到接口，在本示例中选中的宏是“RFID\_Macro1”。该示例假定 VLAN 30 先前已被配置为 RFID VLAN。行 1170 是来自交换机 DC\_Switch1 的命令提示。

返回参考图 10，例如，为了利用现有的 SmartPorts 实现方式配置端口 1020，用户（例如网络管理员）将需要手工进入每个端口，为每个设备选择宏（如果存在的话），并将适当的宏应用到与该设备相连接的端口。例如，用户将需要确定用于与 RFID 读取器 1010 的连接的适当端口配置，确定对于该配置是否存在宏，并且如果存在的话，应用适当的宏来配置端口 1020。如果不存在这样的宏，则端口配置的每个属性将需要被单独指示。

现将参考图 12A 和 12B 描述本发明的一些示例性实现方式。图 12A 是概括根据本发明的方法 1200 的流程图。图 12B 是网络 1250 的简化网络图，其提供了如何实现方法 1200 的一个示例。

本领域的技术人员将意识到，这里论述的方法（包括方法 1200）的一些步骤不需要以所示的顺序来执行（并且在一些实现方式中不被执行）。此外，这里论述的方法的一些实现方式可包括比图 12A 所示的更多或更少的步骤。

类似地，本领域的技术人员将会意识到，图 12B 的元素被简化了，并且只是示例性的。图 12B 示出了交换机 1265、1280 和 1285，它们都具有附接的设备。在本示例中，交换机 1265 是 Cisco Catalyst 4500 系列交换机，交换机 1280 和 1285 是 Cisco Catalyst 3750 系列交换机。但是，本领域的技术人员将会意识到，其他类型的网络设备也可用来实现本发明。此外，交换机 1265、1280 和 1285 可位于相同位置（例如在同一仓库或工厂中），或者可位于不同位置。交换机 1265、1280 和 1285 可经由网络 1275 与 DHCP 服务器 1270、主机设备 1290 和存储设备 1295 通信。因此，网络 1275 可包括一个或多个专用网络的某些部分和因特网的一部分。

附接到交换机 1265、1280 和 1285 的设备不一定要全是相同类型的。在本示例中，设备 1255 是 RFID 读取器，设备 1257 是 IP 电话。如本文别处所论述的，即使是具有相同的一般类型的设备也可具有不同的能力和/或

不同的期望功能。

向 DHCP 服务器发出对 IP 地址的起动的设备通过包括“DHCPDISCOVER”请求的分组来完成这一点。该命令包括设备的介质访问控制（“MAC”）地址，等等。这里通过引用并入 RFC 2131。

因此，在方法 1200 的步骤 1201 中，图 12B 的设备 1255 初始化，然后向交换机 1265 的端口 1260 发送 DHCPDISCOVER 请求 1256。交换机 1265 不仅被配置为经由网络 1275 将 DHCPDISCOVER 请求 1256 转发到 DHCP 服务器 1270，还被配置为分析 DHCPDISCOVER 请求 1256 的内容。交换机 1265 根据方法 1200 执行的步骤可由一个或多个逻辑设备 1268 控制，在本示例中所述逻辑设备是 ASIC。但是，（一个或多个）逻辑设备 1268 可以是任何便利的（一个或多个）逻辑设备。

在步骤 1215 中，交换机 1265 尝试根据 DHCPDISCOVER 请求 1256 中的信息识别设备 1255。在本示例中，交换机 1265 应用“探听（snooping）”技术来分析 DHCPDISCOVER 请求 1256 中的选项的内容。交换机 1265 例如可检查 DHCP 选项 60 的内容，以确定设备类型或厂商标识符。这里通过引用并入 RFC 2132。交换机 1265 可检查 DHCP 选项 125 的“企业号码”字段，以确定设备的 EPCGlobal 企业号码。这里通过引用并入 RFC 3925。

或者（或附加地），交换机 1265 可检查其他 DHCP 选项。例如，交换机 1265 可检查 DHCP 选项 150 以识别设备 1255；该选项例如被 Cisco Systems, Inc. 提供的 IP 电话所使用。R. Johnson 的草案“TFTP Server Address DHCP Option”（Network Working Group（网络工作组），2005 年 2 月 6 日）描述了相关信息，这里通过引用将其并入。交换机 1265 可检查“PXE 引导”选项，以确定端口 1260 的适当配置。M. Johnston 的草案“DHCP Preboot eXecution Environment (PXE) Options”（Dynamic Host Configuration Working Group（动态主机配置工作组），2005 年 1 月 21 日）描述了相关信息，这里通过引用将其并入。交换机 1265 可检查选项 43 以获得关于设备 1255 的因厂商而定的信息。交换机 1265 可检查选项 61 以确定设备 1255 的 EPC 标识符。

在一些实现方式中，交换机 1265 在步骤 1215 中还设备 1255 确定适当的个性。在一些这样的实现方式中，交换机 1265 检查 DHCP 选项 77 以确定设备个性。在其他实现方式中，交换机 1265 可间接地为设备 1255 确定适当的个性，例如通过基于 DHCPDISCOVER 请求 1256 中的其他信息，交叉参考查找表或类似的数据结构来确定。查找表可被存储在本地（例如在存储器 1267 中），存储在附接的设备中，或存储在交换机 1265 可经由网络 1275 访问的另一设备上，其中在本示例中网络 1275 的一部分是因特网。

如果交换机 1265 不能识别设备 1255，则在本示例中过程结束（图 12A 的步骤 1240）。或者（或附加地），可通过使交换机 1265 向主机设备 1290 发送消息来警告网络管理员。

但是，如果交换机 1265 能够识别设备 1255，则方法进行到步骤 1220，在该步骤中，交换机 1265 确定端口 1260 已被配置。（在图 12A 的流程图中，假定已经从宏的应用得到了端口配置（如果有的话），但不一定要是这样）。

如果端口 1260 尚未被配置，则确定是否有适合于设备 1255 的配置宏可用（例如在本地可用或存储在存储器 1267 中）（步骤 1230）。表 1266 是可用于这种目的一种示例性数据结构。表 1266 包括宏字段 1272，用于定义多个配置宏，其中每一个对应于设备 ID 字段 1274 的一个设备。因此，按上文参考步骤 1215 描述的方式（或其他方式）确定的设备 ID 可被用于确定是否有相应的宏。

如果端口 1260 已被配置，则在步骤 1225 中确定配置是否适合于步骤 1215 中识别的设备。如果是，则过程结束。

如果端口不具有期望的配置，则在步骤 1230 中确定是否有可用于设备的适当的宏。如果有可用于设备的适当的宏，则宏被应用（步骤 1235），然后过程结束（步骤 1240）。如果没有，则过程在没有宏被应用的情况下结束。优选地，例如通过从交换机 1265 发送消息到主机设备 1290 来通知网络管理员。

在前述示例中，交换机 1265 具有用于确定如何自动配置在其上接收

DHCPDISCOVER 请求的端口的智能。交换机自身分析 DHCPDISCOVER 请求，并利用适当的属性组合来配置端口。这些属性组合与用于应用它们的必要软件一起，被存储在交换机自身之中。

但是，在本发明的其他实现方式中，用于确定如何适当配置端口的智能以及用于这样配置端口的指令可能都由另一设备拥有。例如，该智能可能存在于 DHCP 服务器 1270、边缘服务管理服务器、认证服务器和专用于端口配置的设备中。一些这样的实现方式由图 13 的流程图示出。

在步骤 1301 和 1305 中，设备初始化并向交换机端口发送 DHCPDISCOVER 请求。在本示例中，交换机 1265 转发 DHCPDISCOVER 请求以及对关于在其上接收 DHCPDISCOVER 请求的端口的指示（步骤 1310）。端口 ID 例如可在 DHCP 选项 82 中提供。优选地，交换机还将关于当前端口配置的信息转发到 DHCP 服务器 1270。

根据一些实现方式，DHCP 服务器 1270 尝试识别设备（步骤 1312）。如果 DHCP 服务器 1270 能识别设备，则 DHCP 服务器 1270 执行步骤 1320、1325 和 1330，这些步骤与方法 1200 的步骤 1220 至 1230 类似。

DHCP 服务器 1270 随后指示交换机 1265 以适当的方式，例如通过应用宏，来配置端口（步骤 1335）。用于此目的的宏（或类似的）可被存储在交换机 1265 中，可被从 DHCP 服务器 1270 发送到交换机 1265，或者可由交换机 1265 从另一设备获得。例如，DHCP 服务器 1270 可向交换机 1265 发送指向其中存储有这种信息的存储器空间（例如在存储设备 1295 之一中）的指针。

在其他实现方式中，DHCP 服务器 1270 响应于 DHCPDISCOVER 请求提供 IP 地址，并将 DHCPDISCOVER 请求转发到执行与步骤 1210 至 1230 类似的步骤的另一个设备。设备例如可以是认证服务器，或者专用于自动端口配置的服务器。该设备可指示交换机 1265 以适当的方式（例如如上所述）来配置端口。

或者，DHCP 服务器 1270 可至少执行设备和端口的识别步骤。DHCP 服务器 1270 随后可将该信息转发到另一个设备，该设备首先执行设备类

型到期望配置的映射，然后指示交换机 1265 相应地配置端口 1260。

在其他实现方式中，交换机 1265 本地的设备执行与步骤 1215 至 1230 类似的步骤，然后相应地指示交换机 1265。例如，交换机 1265 中的 DHCP 中继代理被编程为例如在将 DHCPDISCOVER 请求转发到 DHCP 服务器之前，将 DHCPDISCOVER 请求的拷贝转发到执行与步骤 1210 至 1230 类似的步骤的另一个设备（例如边缘服务管理服务器）。在这种实现方式中，DHCP 服务器可充当常规的 DHCP 服务器，并且交换机 1265 可能没有用于执行步骤 1210 至 1230 的智能。DHCPDISCOVER 请求可被转发到局域网上的执行与步骤 1210 至 1230 类似的步骤的另一个设备。

但是，如图 14 所示，本发明的一些实施例将实现本发明所必需的许多组件组合在单个机箱内。在这里，机箱 1400 是包括交换机模块 1405 的路由器，其中端口 1410 可被配置用于与设备 1415 适当地通信。在本示例中，路由器 1400 还包括 DHCP 服务器 1420，该 DHCP 服务器可实现为软件和/或硬件（例如实现为线路卡或“刀片（blade）”）。在其他一些实现方式中，DHCP 服务器 1420 可实现在与路由器 1400 通信的单独设备中。

本发明的另一些实施例不是被实现在具有交换机模块的路由器中，而是提供了这样一种机箱 1400，该机箱是运行第 3 层运行 IOS 的交换机。同上，机箱 1400 也可包括实现为软件和/或硬件的 DHCP 服务器 1420，或者 DHCP 服务器 1420 可实现在与机箱 1400 通信的单独的设备中。

本领域的技术人员将会意识到，根据本发明的方法可有利地配置其他类型的设备，包括但不限于销售点设备（例如“收银机”）VoIP 电话和制造中所用的设备。例如，一个或多个定义的字段可指示设备类型、设备个性等等。

在一个这样的示例中，DHCP 选项 60 可指示设备是收银机，DHCP 选项 77 可指示收银机的“个性”，例如其是由特定类型的餐馆使用的收银机。可以存在用于为每类设备（例如为收银机）适当配置交换机端口的预定义的宏。



### 其他实施例

虽然这里示出和描述了本发明的示例性实施例和应用，但是许多保持在本发明的概念、范围和精神之内的变化和修改是可能的，并且本领域的技术人员在仔细阅读本申请之后将清楚看出这些变化。

因此，当前的实施例应当被视为示例性的，而不是限制性的，并且本发明并不局限于这里给出的细节，而是可以在所附权利要求的范围和等同物内被修改。

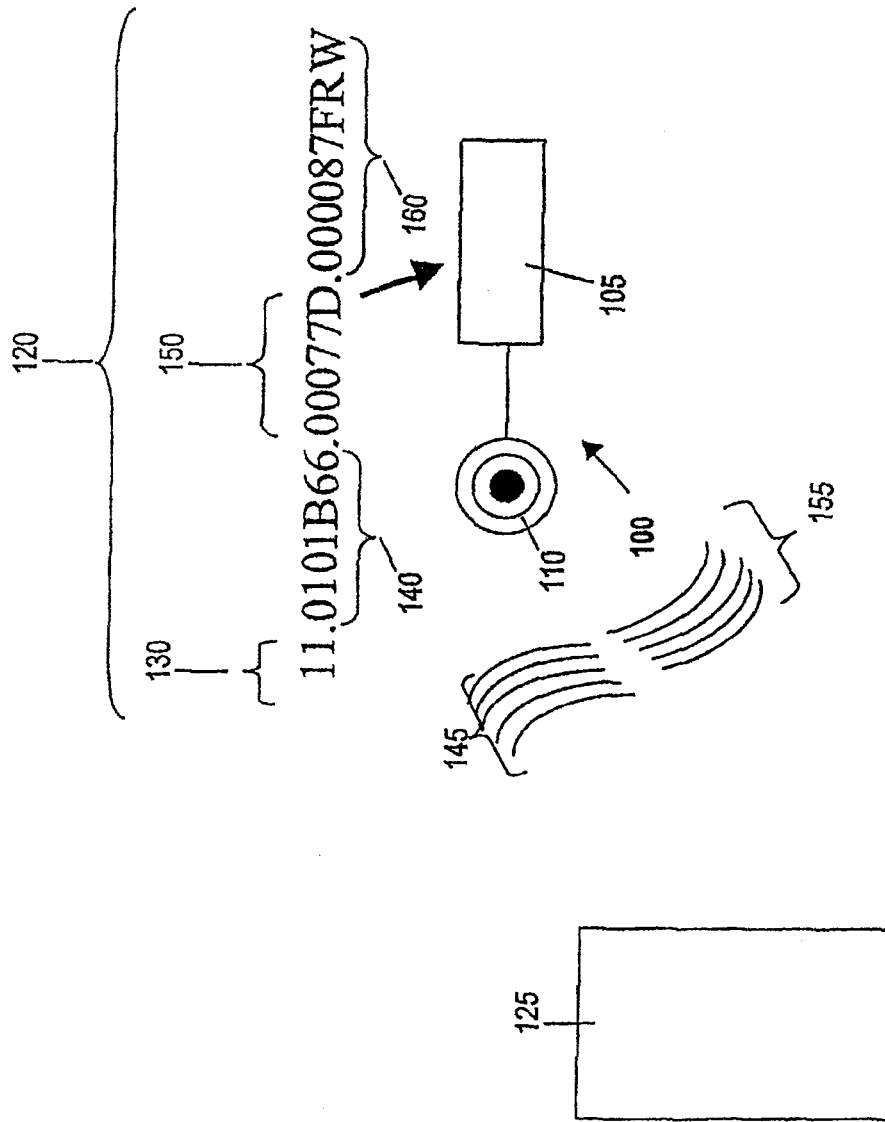


图1

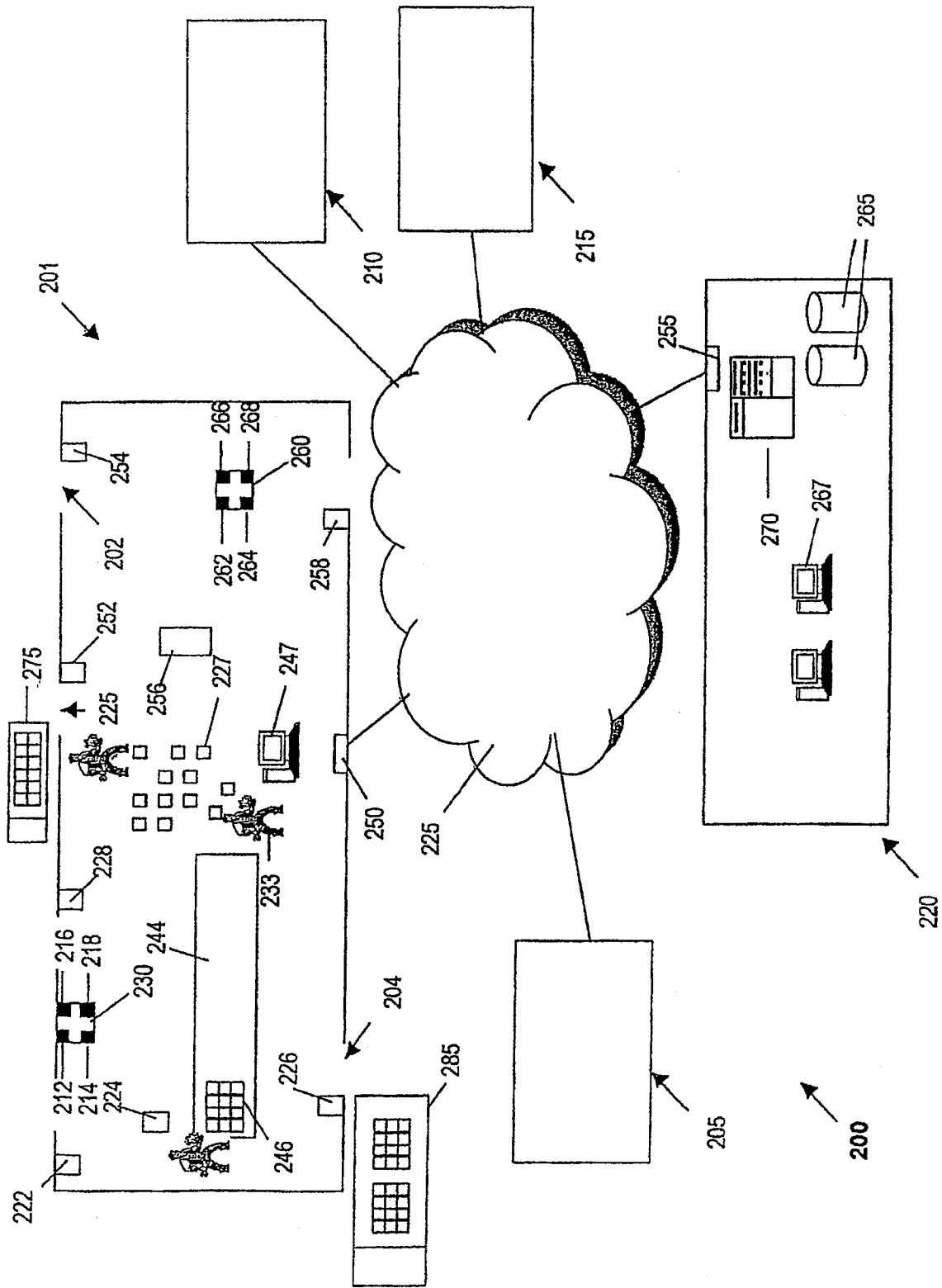


图2

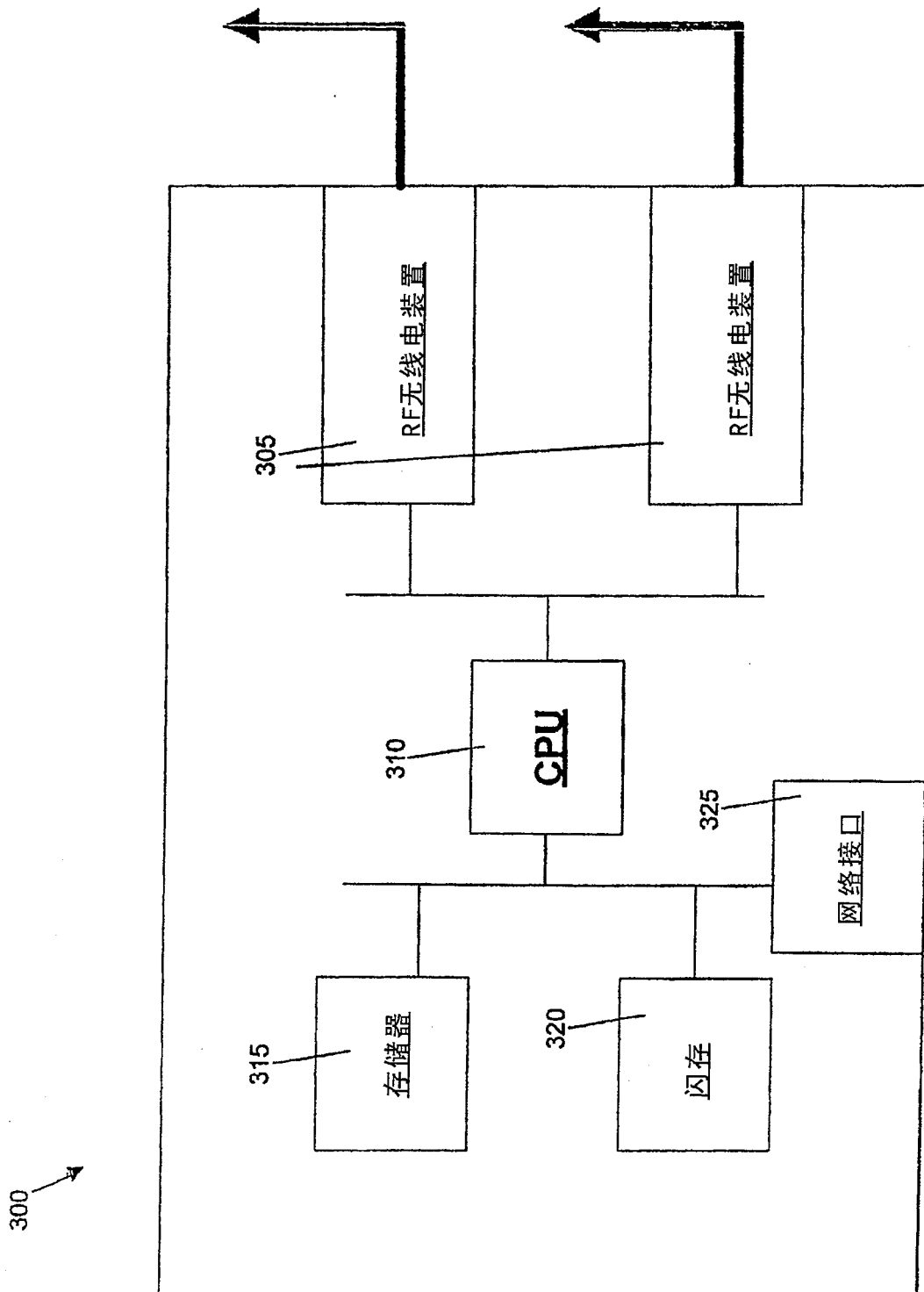


图3

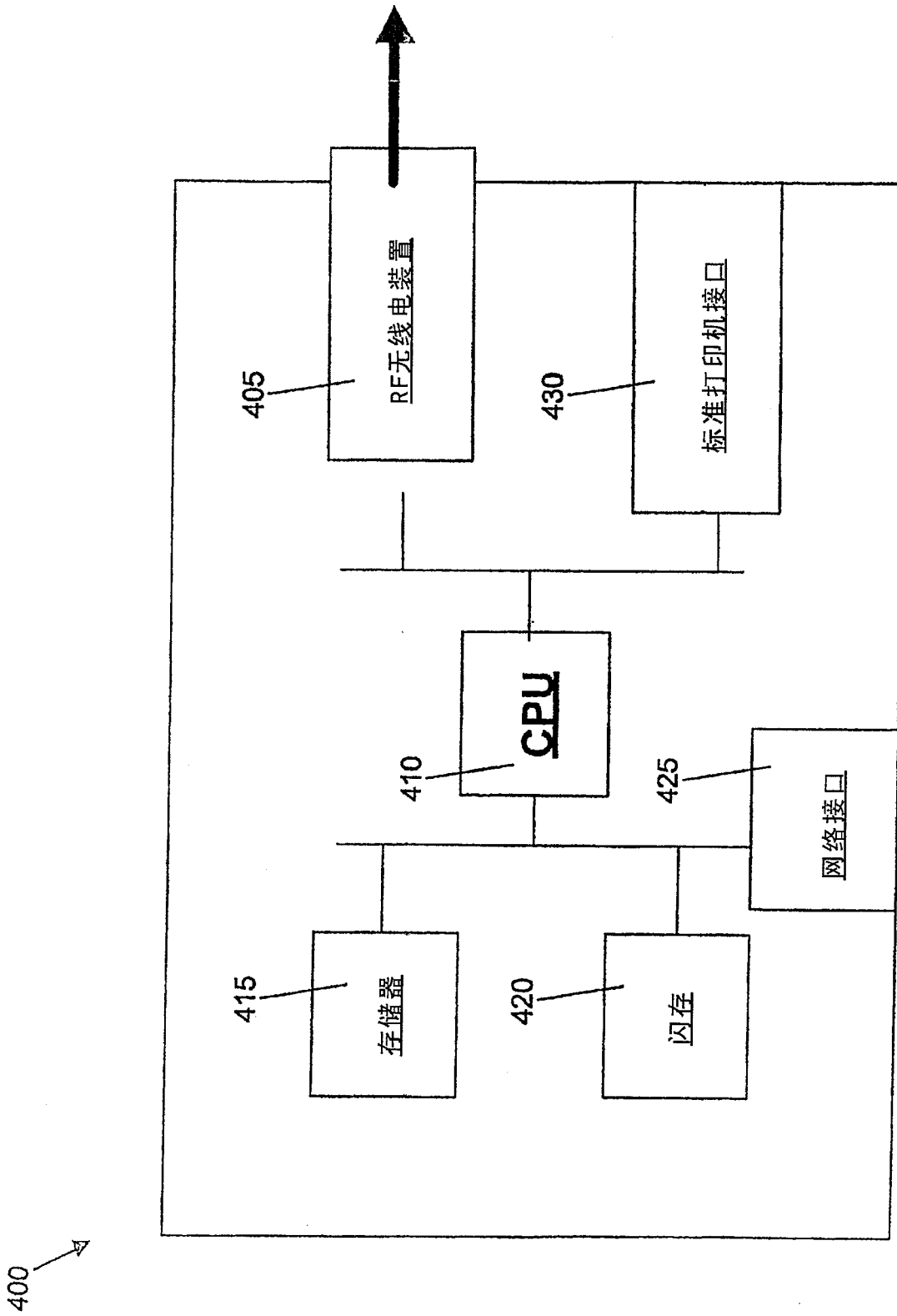


图4

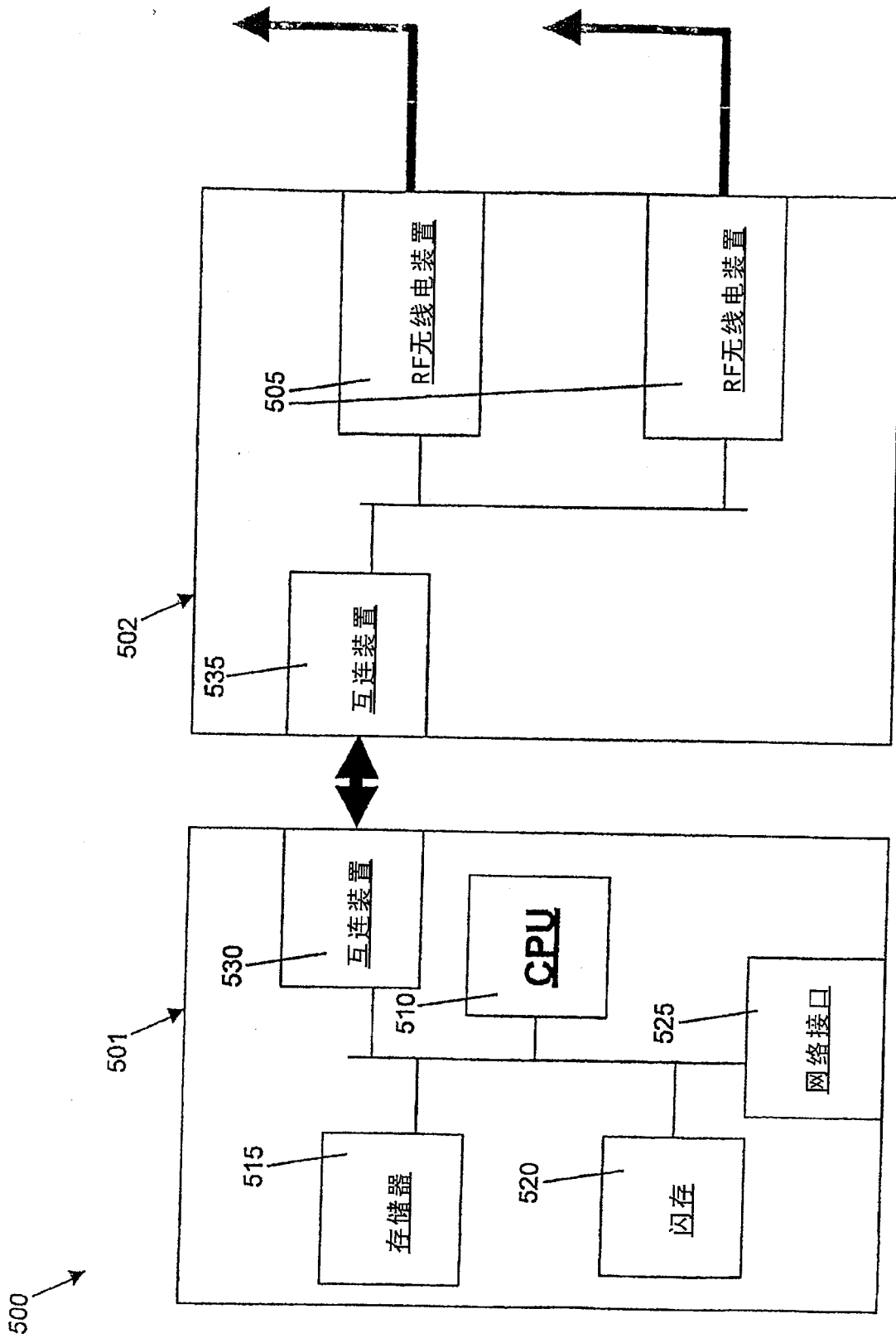


图5

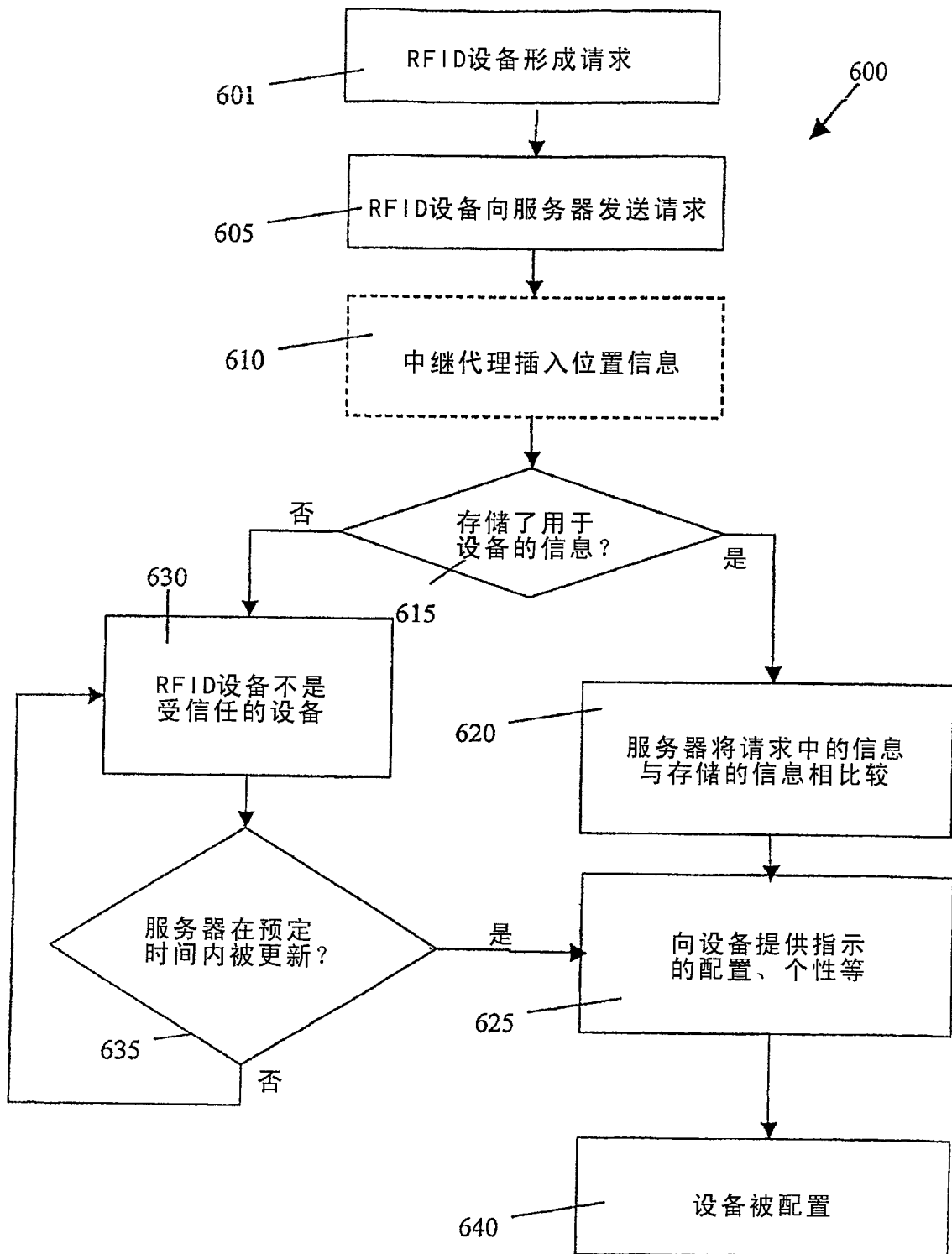


图6

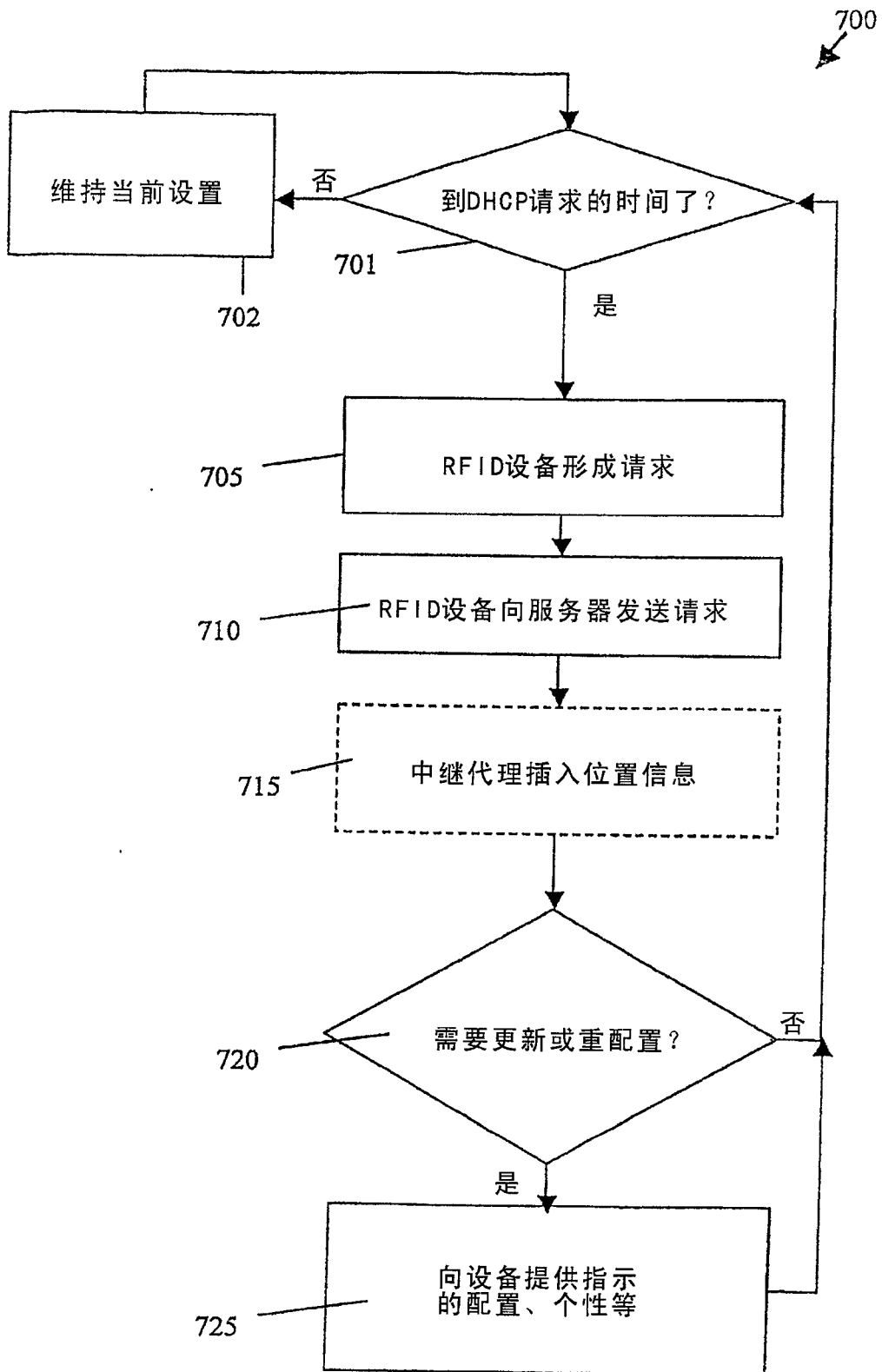


图7



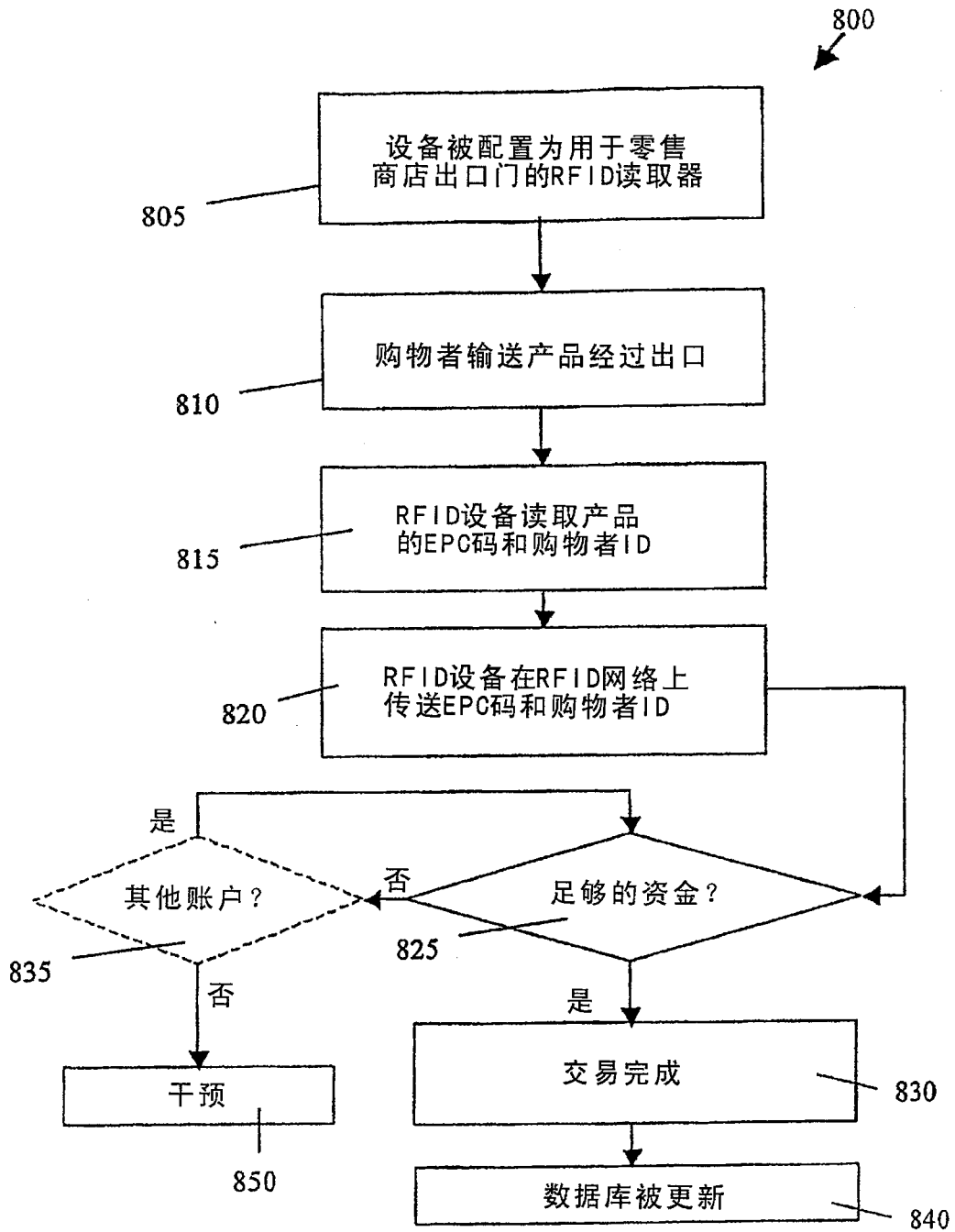


图8

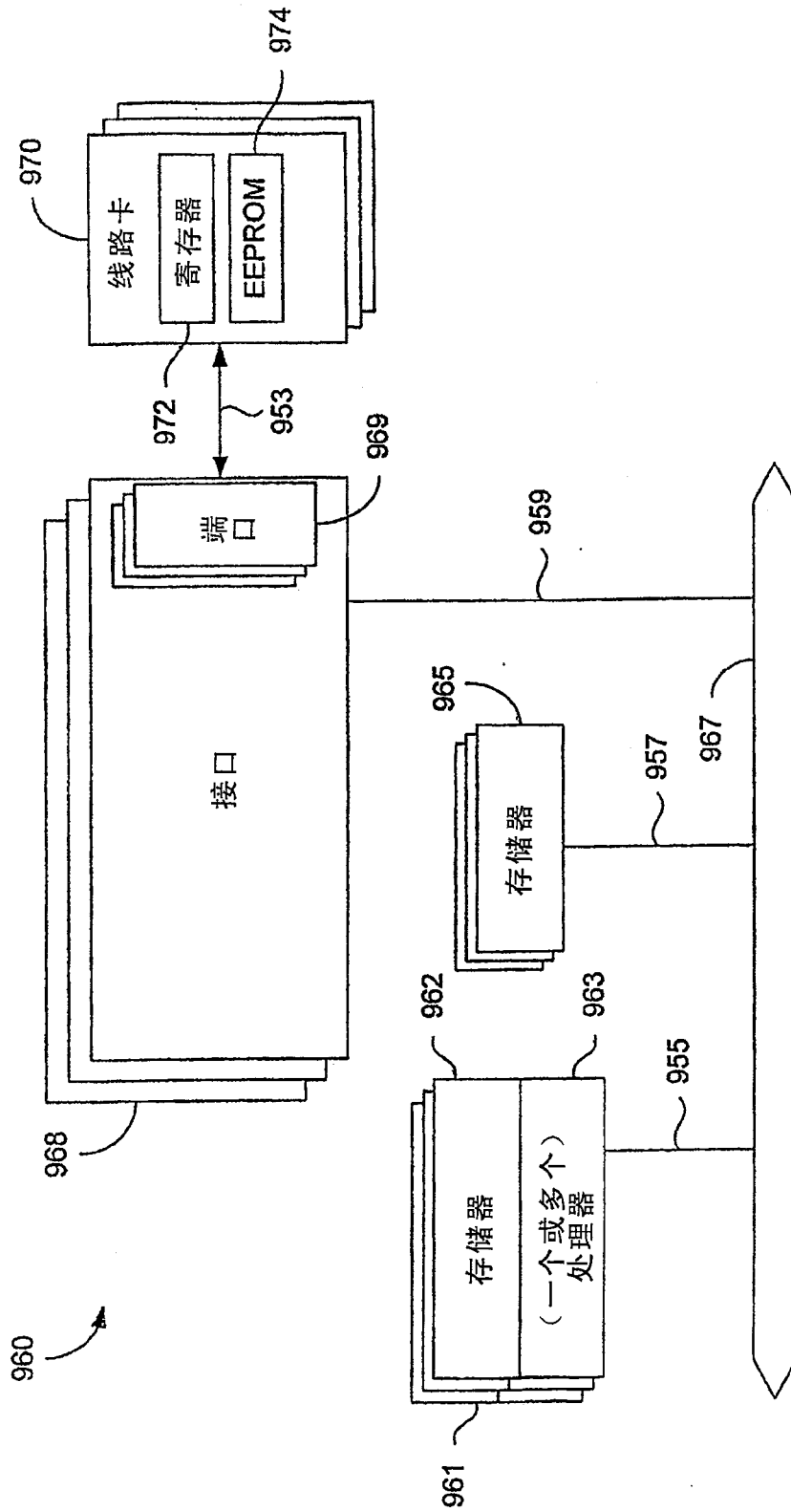


图9

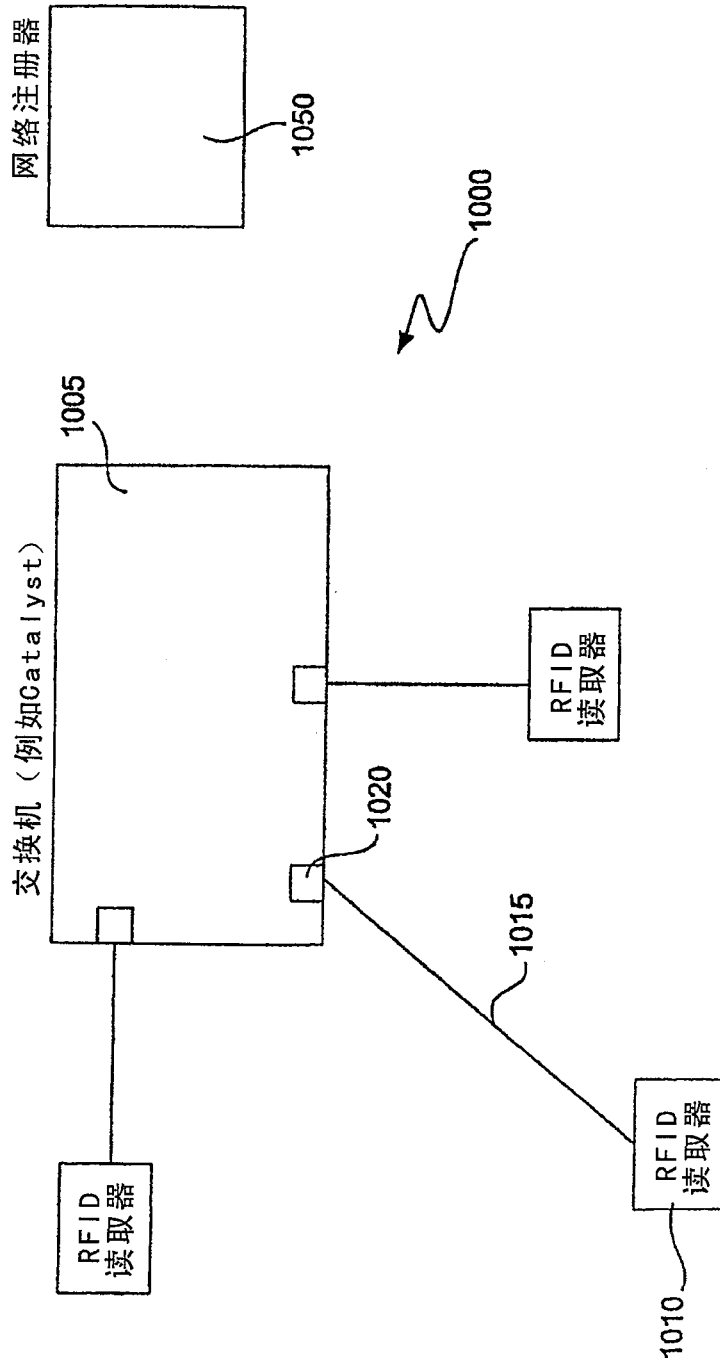


图10

1100 ↙

macro name RFID\_Macro1 ~~~~~ 1101

switchport access vlan \$RFID ~~~~~ 1103

switchport mode access ~~~~~ 1105

description CONNECTION TO RFID DEVICE ~~~~~ 1107

switchport port-security ~~~~~ 1109

switchport port-security maximum 1

switchport port-security violation restrict ~~~~~ 1111

switchport port-security aging time 10 ~~~~~ 1113

switchport port-security aging type inactivity

spanning-tree portfast ~~~~~ 1115

spanning-tree bpduguard enable

storm-control broadcast level 20.0 ~~~~~ 1117

storm-control multicast level 20.0

ip dhcp snooping limit rate 100 ~~~~~ 1119

mls qos trust dscp ~~~~~ 1121

图 11 A

1150

DC\_Switch1# configure terminal 1151

Enter configuration commands, one per line. End with CNTL/Z. 1155

DC\_Switch1(config)# interface FastEthernet0/7 1160

DC\_Switch1(config-if)# macro apply RFID\_Macro1 \$RFID 30 1165

DC\_Switch1(config-if)# 1170

图 11 B

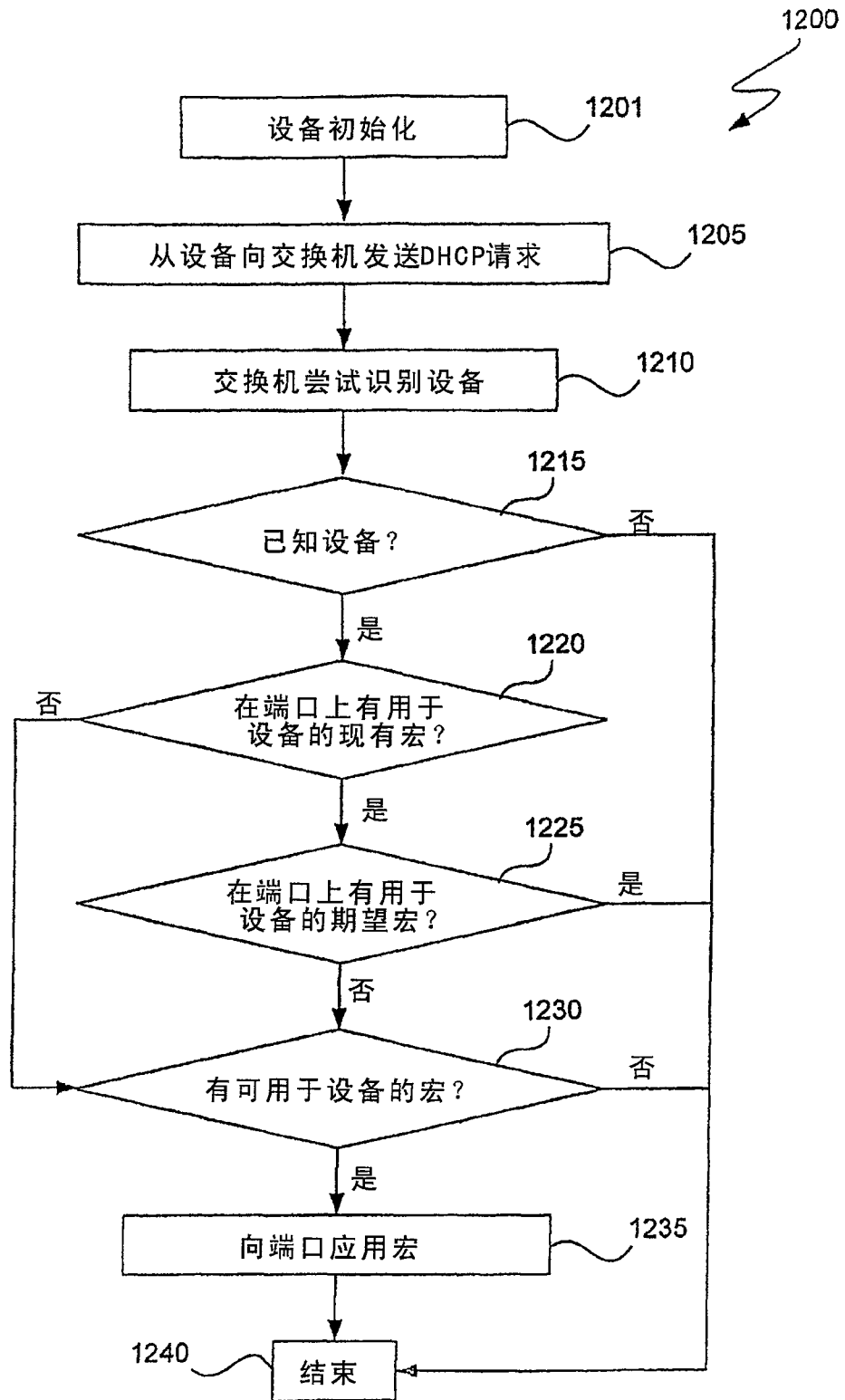


图12A

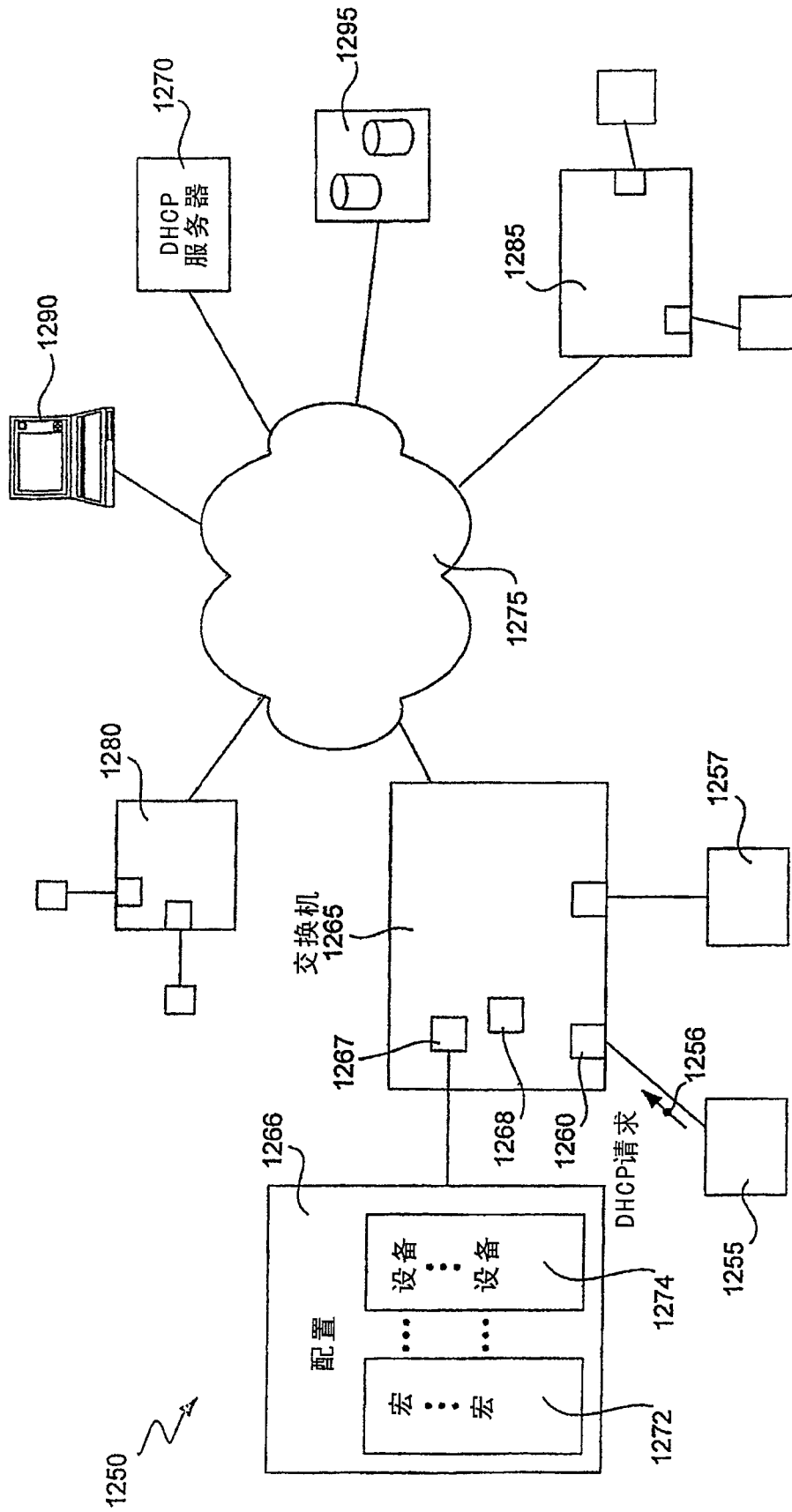


图12B

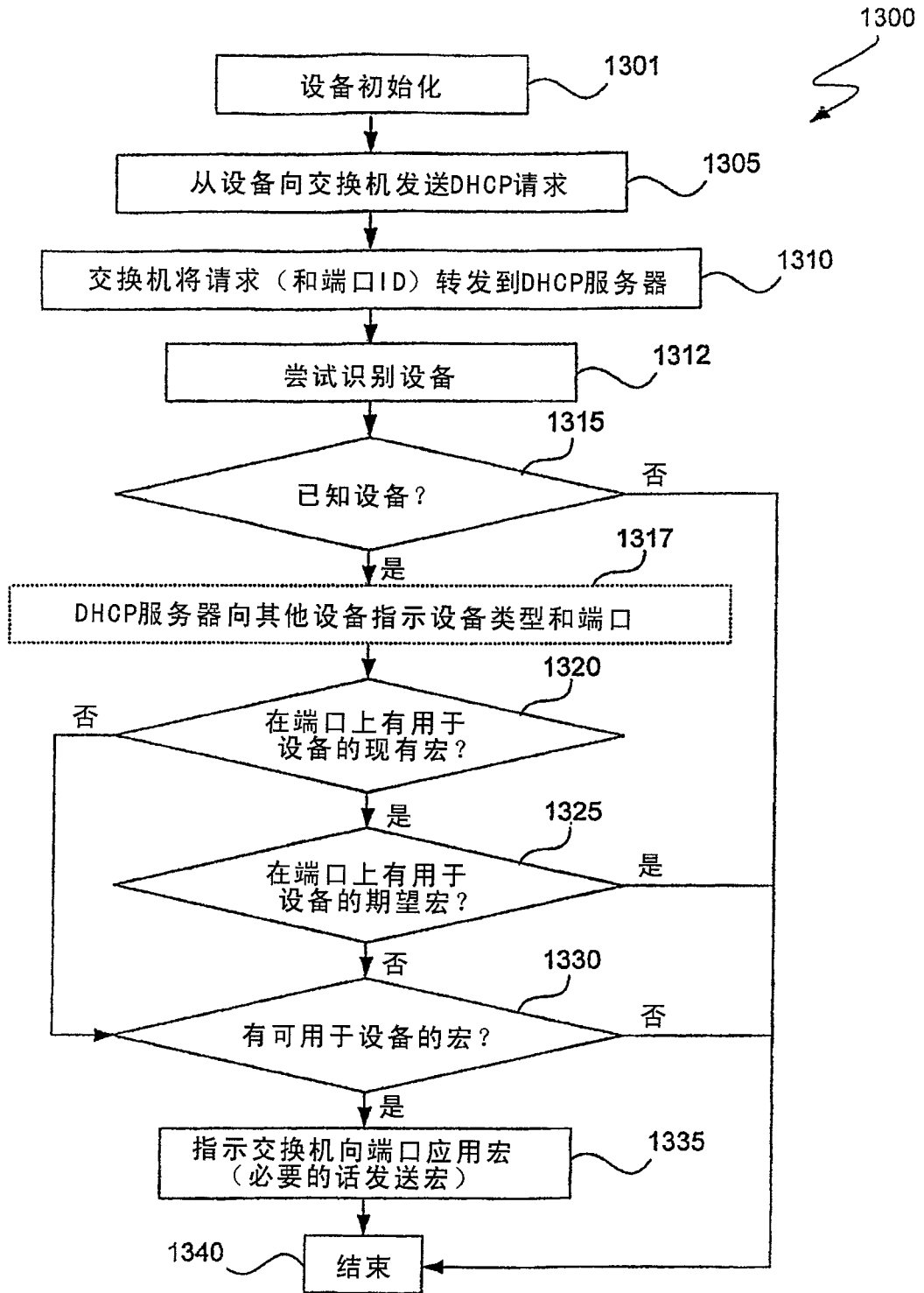


图13



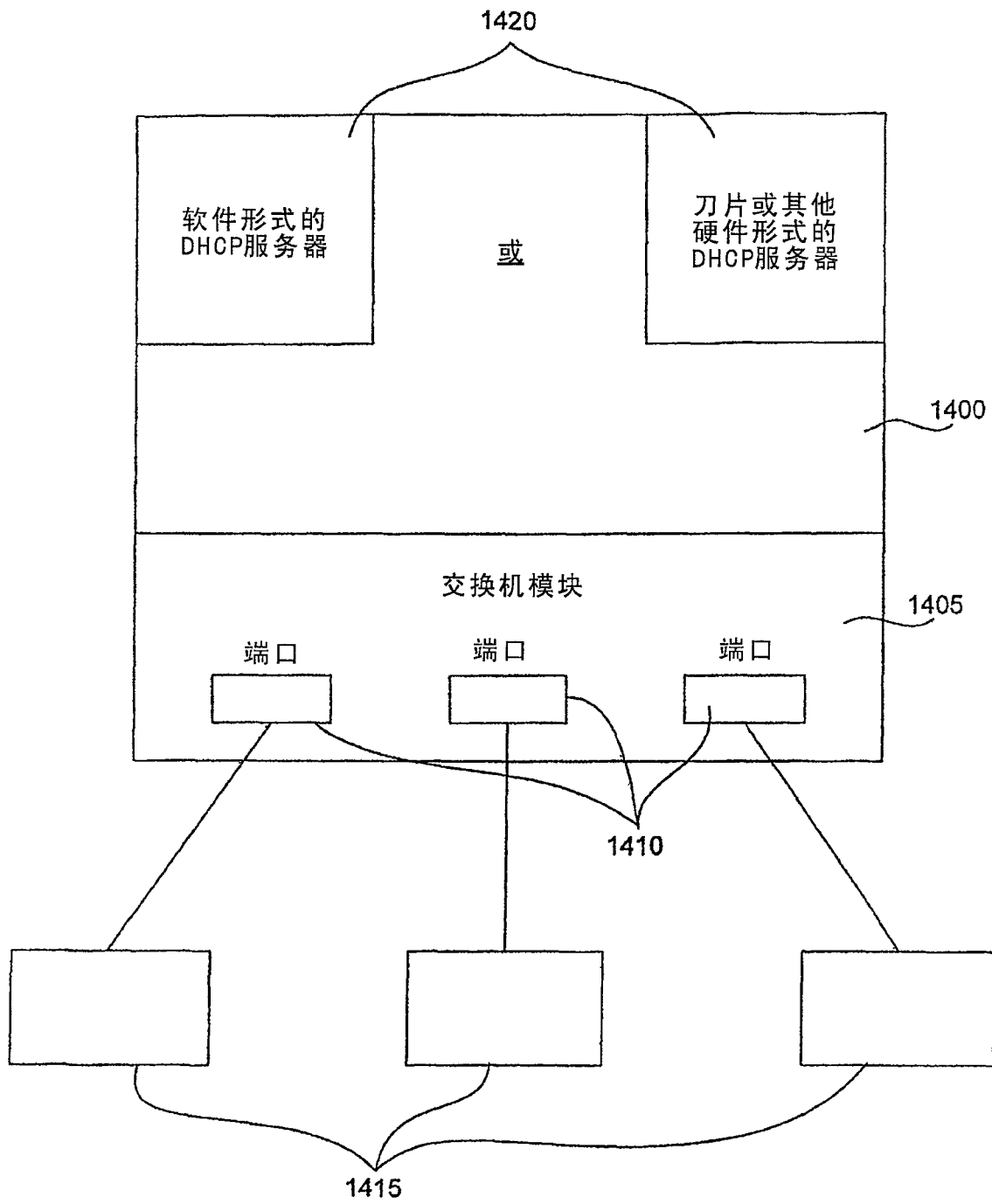


图14