(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111385139 A
(43)申请公布日 2020.07.07

(21)申请号 201910569721.7

(22)申请日 2019.06.27

(30)优先权数据
16/234,379 2018.12.27 US

(71)申请人 瞻博网络公司
地址 美国加利福尼亚州

(72)发明人 K·A·沃森 G·弗德考乌

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 酆迅 姚杰

(51)Int.Cl.
H04L 12/24(2006.01)
H04L 29/06(2006.01)
H04L 29/12(2006.01)

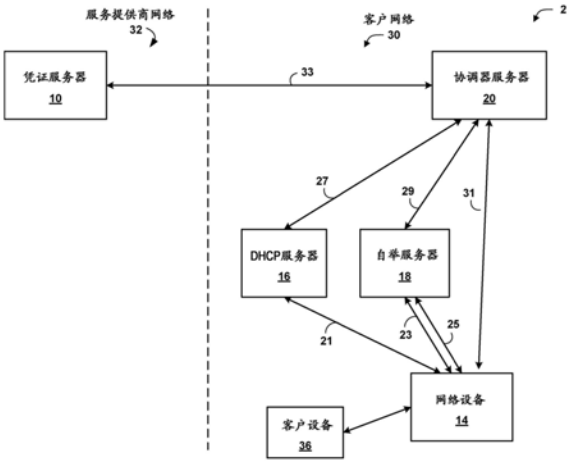
权利要求书3页 说明书15页 附图4页

(54)发明名称

网络设备的安全远程自举

(57)摘要

公开了用于执行网络设备的安全远程自举操作使得敏感配置驻留在易失性存储器中或者在断电时是不可访问的技术。在一个示例中,网络设备执行针对导引信息的第一请求。响应于确定网络设备的第一初始化还没有发生,网络设备通过利用导引信息配置网络设备以将文件系统的一部分安装到易失性存储器而非非易失性存储器来执行第一初始化。在重新启动后,网络设备执行针对导引信息的第二请求。响应于确定网络设备的第一初始化已经发生,网络设备执行网络设备的自举操作。自举操作可以将网络设备配置为用于远程管理,使得远程获得的任意后续配置在断电时不被保留。



CN 111385139 A

1.一种方法,包括:

由网络设备的一个或多个处理器执行针对所述网络设备的导引信息的第一请求;

由所述一个或多个处理器处理所述导引信息,以确定所述网络设备的第一初始化还没有发生;

响应于确定所述网络设备的所述第一初始化还没有发生,通过以下各项执行所述第一初始化:

由所述一个或多个处理器利用所述导引信息配置所述网络设备以将文件系统的至少一部分挂载到所述网络设备的易失性存储器,而不是所述网络设备的非易失性存储器;以及

由所述一个或多个处理器重新启动所述网络设备;

在重新启动所述网络设备之后:

由所述一个或多个处理器执行针对所述网络设备的所述导引信息的第二请求;

由所述一个或多个处理器处理所述导引信息,以确定所述网络设备的所述第一初始化已经发生;以及

响应于确定所述网络设备的所述第一初始化已经发生,由所述一个或多个处理器执行所述网络设备的自举操作。

2.根据权利要求1所述的方法,还包括:在重新启动所述网络设备之后,将所述文件系统的所述至少一部分挂载到所述网络设备的所述易失性存储器。

3.根据权利要求2所述的方法,还包括:

在将所述文件系统的所述至少一部分挂载到所述网络设备的所述易失性存储器之后,在所述网络设备断电时,从所述网络设备的所述易失性存储器中失去所述文件系统的至少一部分。

4.根据权利要求1所述的方法,其中执行所述网络设备的所述自举操作包括:配置所述网络设备以用于由第二网络设备进行远程管理。

5.根据权利要求4所述的方法,其中配置所述网络设备以用于由所述第二网络设备进行远程管理包括:处理所述导引信息以获得主机名、网络地址、端口、网络协议、或者所述第二网络设备的安全证书中的一个或多个。

6.根据权利要求4所述的方法,其中配置所述网络设备以用于由所述第二网络设备进行远程管理包括:由所述网络设备基于所述导引信息来初始化与所述第二网络设备的远程通信会话。

7.根据权利要求1所述的方法,其中执行所述网络设备的所述自举操作包括:利用一次性密钥加密所述网络设备的所述非易失性存储器的交换空间。

8.根据权利要求1所述的方法,

其中所述网络设备是第一网络设备,

其中执行针对所述网络设备的所述导引信息的所述第一请求包括:经由第一非接触式供应操作来从一个或多个网络设备请求所述第一网络设备的所述导引信息,以及

其中执行针对所述网络设备的所述导引信息的所述第二请求包括:经由第二非接触式供应操作来从所述一个或多个网络设备请求所述第一网络设备的所述导引信息。

9.根据权利要求8所述的方法,其中所述第一非接触式供应操作和第二非接触式供应

操作是第一零接触供应(ZTP)操作和第二零接触供应(ZTP)操作。

10.根据权利要求8所述的方法,还包括:

在经由所述第一非接触式供应操作来请求所述第一网络设备的所述导引信息之前,由所述一个或多个处理器从动态主机配置协议(DHCP)服务器经由第三非接触式供应操作请求用于所述一个或多个网络设备的地址信息。

11.根据权利要求1所述的方法,其中执行所述第一初始化还包括:由所述一个或多个处理器配置对所述网络设备的本地用户访问许可。

12.根据权利要求11所述的方法,其中配置对所述网络设备的所述本地用户访问许可包括以下至少一项:

由所述一个或多个处理器禁用所述网络设备的一个或多个控制台端口;或者

由所述一个或多个处理器设置用于对所述网络设备的根访问的密码。

13.根据权利要求11所述的方法,其中配置对所述网络设备的所述本地用户访问许可还包括:将对所述网络设备的所述本地用户访问许可存储在所述网络设备的所述非易失性存储器中而不是所述网络设备的所述易失性存储器中。

14.一种网络设备,包括:

非易失性存储器;

易失性存储器;以及

一个或多个处理器,被配置为:

执行针对所述网络设备的导引信息的第一请求;

处理所述导引信息以确定所述网络设备的第一初始化还没有发生;

响应于确定所述网络设备的所述第一初始化还没有发生,通过以下项执行所述第一初始化:

利用所述导引信息配置所述网络设备,以将文件系统的至少一部分挂载到所述易失性存储器而不是所述非易失性存储器;以及

重新启动所述网络设备;

在重新启动所述网络设备后:

执行针对所述网络设备的所述导引信息的第二请求;

处理所述导引信息以确定所述网络设备的所述第一初始化已经发生;以及

响应于确定所述网络设备的所述第一初始化已经发生,

执行所述网络设备的自举操作。

15.根据权利要求14所述的网络设备,其中所述一个或多个处理器还被配置:为在重新启动所述网络设备之后,将所述文件系统的至少一部分挂载到所述网络设备的所述易失性存储器。

16.根据权利要求15所述的网络设备,其中在将所述文件系统的所述至少一部分挂载到所述网络设备的所述易失性存储器之后,所述网络设备还被配置为在所述网络设备断电时,从所述易失性存储器中失去所述文件系统的所述至少一部分。

17.根据权利要求14所述的网络设备,其中为了执行所述网络设备的所述自举操作,所述一个或多个处理器还被配置为:配置所述网络设备以用于由第二网络设备进行远程管理。

18.根据权利要求14所述的网络设备，其中为了执行所述网络设备的所述自举操作，所述一个或多个处理器还被配置为用一次性密钥加密所述网络设备的所述非易失性存储器的交换空间。

19.根据权利要求14所述的网络设备，

其中所述网络设备是第一网络设备，

其中为了执行针对所述网络设备的所述导引信息的所述第一请求，所述一个或多个处理器被配置为经由第一非接触式供应操作从一个或多个网络设备请求所述第一网络设备的所述导引信息，并且

其中为了执行针对所述网络设备的所述导引信息的所述第二请求，所述一个或多个处理器被配置为经由第二非接触式供应操作从所述一个或多个网络设备请求所述第一网络设备的所述导引信息。

20.一种非暂态计算机可读介质，包括指令，所述指令被配置为使得网络设备的一个或多个处理器用于：

执行针对所述网络设备的导引信息的第一请求；

处理所述导引信息以确定所述网络设备的第一初始化还没有发生；

响应于确定所述网络设备的所述第一初始化还没有发生，通过以下项来执行所述第一初始化：

利用所述导引信息来配置所述网络设备，以将文件系统的至少一部分挂载到所述网络设备的易失性存储器中而不是所述网络设备的非易失性存储器中；以及

重新启动所述网络设备；

在重新启动所述网络设备后：

执行针对所述网络设备的所述导引信息的第二请求；

处理所述导引信息以确定所述网络设备的所述第一初始化已经发生；以及

响应于确定所述网络设备的所述第一初始化已经发生，执行所述网络设备的自举操作。

网络设备的安全远程自举

技术领域

[0001] 本公开一般涉及网络设备，并且更具体地，涉及网络设备的部署和激活

背景技术

[0002] 大型企业经常面临网络基础设施的大规模分发和部署的挑战。例如企业可以操作许多地理上分布的设施(例如办公室、零售店等)，这些设施需要网络连接到企业的中央或主要办公室并且可选地彼此连接。在这种情况下，当企业希望使用许多远程设施中的每一个来安装或升级网络设备时，就会出现挑战。例如企业的中央信息技术(IT)管理组可以协调用于升级远程设施中的每一个的计算机、防火墙、网关、路由器、VPN应用、交换机或其他网络设备的工作。这种操作可能需要数百或者有时数千个设备的部署和激活。

[0003] 为了简化该过程，企业可以在一次大规模的展示(“mass rollout”)中购买用于在远程设施处部署的类似网络设备。通过购买类似的如果不是相同的网络设备，企业可以减轻关于部署和操作这些网络设备的管理负担。在这种情况下，企业通常与制造商签订合同，以将单元直接运送到远程设施。这节省了运输成本并且提供了减轻中央IT组承担物理接收和重新装载设备的负担的优点。但是，当设备直接从制造商运送到设备要被部署的最终位置时，经训练的网络管理员可能常无法总是物理操纵设备以确保正确安装和激活。因此，配置设备的人通常是商店经理或其他没有配置网络设备经验的人。在这种情况下，可能难以确保以以下方式使设备被正确地部署和激活：以便匹配通常由IT组维护的集中式设备管理系统，以用于远程监视和管理企业中的设备。

发明内容

[0004] 通常，本公开描述了用于执行网络设备的安全远程自举操作的技术。为了降低将网络设备配置给不熟练的用户的技术复杂性，传统设备可以使用零接触供应(ZTP)来远程地并自动地执行网络设备的第一次配置以供在企业网络内使用。有关ZTP协议的更多信息在https://tools.ietf.org/html/draft-ietf-netconf-zerotouch中可用的“Zero Touch Provisioning for Networking Devices,”Internet-Draft,Internet Engineering Task Force(IETF)中描述。

[0005] 然而，部署到公共场所(例如售货亭、购物中心、办公室、公寓地下室)的网络设备仍然可能易受具有对设备的物理访问的恶意行为者的攻击。例如传统网络设备可以在网络设备的非易失性存储器内存储敏感信息，诸如用户数据和证书、网络业务、或企业网络内的其他设备的地址和身份。具有对网络设备的物理访问的恶意行为者可能可以移除非易失性存储器并从存储在非易失性存储器上的数据的分析中收集有价值的信息。一种可能的解决方案是配置网络设备以将这种敏感信息存储在网络设备的易失性存储器内，使得敏感信息在设备断电时丢失。然而，这可能超出了依赖于ZTP来执行网络设备的第一次配置的最终用户的能力。此外，应该在非易失性存储器中执行一些安全配置，以防止断电时移除安全配置，进一步增加了最终用户的技术负担。

[0006] 因此，公开了用于执行网络设备的安全远程自举操作的技术，使得敏感信息仅存储在网络设备的易失性存储器上。例如如本文所述的网络设备可以在初始引导周期期间执行第一非接触式供应操作以取回导引信息。网络设备可以处理导引信息以确定网络设备的第一初始化是否已经发生。如果第一初始化没有发生，则网络设备执行第一初始化。例如网络设备可以通过配置本地用户访问许可并将其自身配置为将文件系统的至少一部分挂载到网络设备的易失性存储器而不是网络设备的非易失性存储器来执行第一初始化。此外，网络设备重新启动其自身。

[0007] 对于每个后续引导周期，网络设备将文件系统的至少一部分挂载到易失性存储器和/或加密非易失性存储器的至少一部分。此外，网络设备执行第二非接触式供应操作以请求导引信息。网络设备处理导引信息以确定网络设备的第一初始化是否已经发生。响应于确定第一初始化已经发生，网络设备执行自举操作。作为自举操作的示例，网络设备可以将其自身配置为由另一网络设备进行远程管理。

[0008] 因此，通过使用本公开的技术，网络设备可以执行安全的远程自举操作。此外，在网络设备断电时，网络设备失去存储在易失性存储器上的信息或对存储在非易失性存储器上的加密信息的访问。因此，网络设备不保留可能对具有对网络设备的物理访问的恶意行动者有用的任意信息。因此，本公开的技术为计算机相关的网络设备部署和配置领域提供了特定的技术改进。例如本公开的技术可以允许部署到网络设备的公共空间，该网络设备被保护免去受到恶意行为者的物理或本地攻击。此外，本公开的技术可以允许对非接触式供应的使用来安全地和远程地配置网络设备。另外，本公开的技术可以降低最终用户部署和配置网络设备以在企业网络内操作的成本和技术负担。

[0009] 在一个示例中，本公开描述了一种方法，包括：由网络设备的一个或多个处理器执行针对网络设备的导引信息的第一请求；所述一个或多个处理器处理所述导引信息，以确定所述网络设备的第一初始化还没有发生；响应于确定网络设备的第一初始化还没有发生，通过以下各项执行第一初始化：由一个或多个处理器并使用导引信息，配置网络设备以将文件系统的至少一部分挂载到网络设备的易失性存储器，而不是网络设备的非易失性存储器；并且由一个或多个处理器重新启动网络设备；在重新启动网络设备之后：由一个或多个处理器执行针对网络设备的导引信息的第二请求；所述一个或多个处理器处理所述导引信息，以确定所述网络设备的第一初始化已经发生；并且响应于确定网络设备的第一初始化已经发生，由一个或多个处理器执行网络设备的自举操作。

[0010] 在另一示例中，本公开描述了一种网络设备，包括：非易失性存储器；易失性存储器；一个或多个处理器，被配置用于：执行针对网络设备的导引信息的第一请求；处理导引信息以确定网络设备的第一初始化还没有发生；响应于确定网络设备的第一初始化还没有发生，通过以下各项执行第一初始化：利用导引信息配置网络设备以将文件系统的至少一部分挂载到易失性存储器而不是非易失性存储器；并重新启动网络设备；在重新启动网络设备后：执行针对网络设备的导引信息的第二次请求；处理导引信息以确定网络设备的第一初始化已经发生；并且响应于确定网络设备的第一初始化已经发生，执行网络设备的自举操作。

[0011] 在另一示例中，本公开描述了一种非暂态计算机可读介质，包括指令，该指令被配置为使网络设备的一个或多个处理器用于：执行针对网络设备的导引信息的第一请求；处

理导引信息以确定网络设备的第一初始化还没有发生;响应于确定网络设备的第一初始化还没有发生,通过以下各项执行第一初始化:利用导引信息来配置网络设备以将文件系统的至少一部分挂载到网络设备的易失性存储器中而不是网络设备的非易失性存储器;并重新启动网络设备;在重新启动网络设备后:执行对网络设备的导引信息的第二次请求;处理导引信息以确定网络设备的第一初始化已经发生;并且响应于确定网络设备的第一初始化已经发生,执行网络设备的自举操作。

[0012] 在附图和以下描述中阐述了本公开的技术的一个或多个示例的细节。

附图说明

[0013] 图1是示出了根据本公开的技术的用于执行安全远程自举操作的示例系统的框图。

[0014] 图2是示出了根据本公开的技术的示例网络设备的框图。

[0015] 图3是示出了根据本公开的技术的示例服务器的框图。

[0016] 图4是示出了根据本发明的技术的示例安全远程自举操作的流程图。

[0017] 在整个附图和描述中,类似的附图标记指代类似的元件。

具体实施方式

[0018] 图1是示出了根据本公开的技术的用于执行安全远程自举操作的示例系统2的框图。通常,本公开描述了用于安全地和远程地配置网络设备14的技术。为了利用集中管理系统(例如协调器服务器20和凭证服务器10)来部署和管理网络设备14,网络设备14请求网络设置、管理配置、上电时自动进行安全配置。根据本公开的技术,网络设备14从例如自举服务器18接收配置信息和引导映像。

[0019] 在图1的示例中,系统2可以包括多个子网络,例如服务提供商网络32和客户网络30。服务提供商网络32向客户网络30提供可用于由客户网络30内的客户设备36请求和使用的网络服务。如下面将更详细讨论的,服务提供商网络32经由凭证服务器10向客户网络30提供认证和验证服务。在一些示例中,服务提供商网络32是因特网服务提供商(ISP),其为客户网络30提供对诸如例如因特网的一个或多个外部网络的访问。

[0020] 客户网络30可以对应于例如零售店或公司部门(例如法律、工程、营销、销售、会计等)。客户网络30可以对应于要为其启用新网络设备14的新子网络。客户网络30包括协调器服务器20,协调器服务器20管理:客户网络30内的每个网络元件(例如路由器,交换机,网关,VPN设备,防火墙等);向客户网络30内的设备提供DHCP服务的DHCP服务器16;向客户网络30内的设备提供配置和自举服务的自举服务器18;一个或多个客户设备36;以及向客户设备36提供网络业务路由和转发服务的网络设备14。为了便于讨论,客户网络30被描绘为包括单个网络设备14、单个DHCP服务器16和单个自举服务器18。然而,在本公开的技术的其他示例中,客户网络30包括多个网络设备14、多个DHCP服务器16、多个自举服务器18或其某种组合。

[0021] 协调器服务器20通信地耦合到客户网络30的网络设备14。协调器服务器20可以从服务提供商网络32的凭证服务器10获得所有权凭证33,如下面更详细描述的。协调器服务器20可以向DHCP服务器16提供DHCP配置27以使DHCP服务器16能够向客户网络30内的诸如

网络设备14的设备提供DHCP服务。另外，协调器服务器20可以向自举服务器18提供自举配置信息29以使自举服务器18能够向网络设备14提供自举服务。一旦网络设备14被部署并激活，协调器服务器20就可以使用诸如NETCONF的通信协议来管理网络设备14。管理的网络设备14在本文也称为网络“元件”。在通常的实践中，由协调器服务器20管理的协调器服务器20和网络设备14由客户的IT组集中维护，并被统称为元素管理系统(EMS)或网络管理系统(NMS)。管理员可以与协调器服务器20交互以远程监视和配置网络设备14。例如管理员可以从协调器服务器20接收关于网络设备14的警报，查看网络设备14的配置或管理数据，修改网络设备14的配置或管理数据，将新的网络设备添加到客户网络30，从客户网络30移除现有的网络设备14，或以其他方式操纵客户网络30和网络设备14。在一些示例中，协调器服务器20为管理员提供设备管理接口(DMI)，以在网络设备14变为活动时管理网络设备14。DMI可以包括诸如图形用户界面(GUI)或命令行界面的界面，管理员通过该界面动态地调整网络设备14或由协调器服务器20管理的其他设备的配置数据。

[0022] DHCP服务器16向客户网络30内的设备提供DHCP服务，诸如网络设备14、自举服务器18和客户设备36。如本文所述，网络设备14可以经由非接触式供应操作来从DHCP服务器16请求自举数据，以执行网络设备14的自动配置。例如网络设备14可以请求来自DHCP服务器16的网络分配以及将网络设备14重定向到自举服务器18以用于导引信息的重定向信息。在一些示例中，非接触式供应操作是ZTP操作。

[0023] 自举服务器18可以用作网络设备14的导引信息的源。如本文所述，网络设备14可以经由非接触式供应操作从自举服务器18请求导引信息以执行网络设备14的自动配置。一些示例，非接触式供应操作是ZTP操作。在一些示例中，自举服务器18是实现YANG模块的RESTCONF服务器。

[0024] 网络设备14通常是对于没有经验的非技术用户来说可能难以操作的网络设备。例如网络设备14通常不包括键盘、监视器或其他传统用户界面。因此，当启动网络设备14时通常不能访问控制台。网络设备14可以对应于例如路由器、交换机、网关、集线器、服务器、计算设备、计算终端、打印机、防火墙、入侵检测和/或防止设备、无线接入点(AP)或其他类型的网络设备。诸如商店经理的没有经验的用户可能难以手动配置网络设备14。因此，本公开的技术可以通过使用安全非接触式供应操作来简化配置网络设备14的过程，安全非接触式供应操作由网络设备14用于在引导周期期间配置其自身，在引导周期时输入控制台通常不可用。

[0025] 引导周期通常是过程，在该过程期间，诸如网络设备14之一的设备的处理器“自举”操作系统内核的加载。通常，处理器包括硬编码指令，该硬编码指令用于在初始接收功率之后，即在设备最初开启之后从定义的存储器地址取回引导加载器。引导加载器包括用于加载内核以及用于初始化诸如各种寄存器值的变量的自举指令。在一些示例中，引导加载器可以包括用于执行非接触式供应操作以取回用于加载内核和/或为网络设备4挂载文件系统的导引信息的指令。

[0026] 客户设备36可以是例如个人计算机、膝上型计算机或与客户网络30的用户相关联的其他类型的计算设备。客户设备36的附加示例包括移动电话、具有例如3G或4G无线卡的膝上型或台式计算机、无线功能上网本、视频游戏设备、寻呼机、智能电话、个人数据助理(PDA)、诸如电视机的物联网(IoT)设备、冰箱、灯泡、恒温器、家庭安全系统、婴儿监视器等。

客户设备36中的每一个可以运行各种软件应用，诸如文字处理和其他办公支持软件、web浏览软件、支持语音呼叫的软件、视频游戏、视频会议和电子邮件等。客户设备36经由有线和/或无线通信链路连接到客户网络30。本文使用的术语“通信链路”包括任意形式的有线或无线传输介质，并且可以包括中间节点，诸如网络设备，诸如网络设备14。

[0027] 根据本公开的技术，公开了网络设备的安全远程自举操作，使得敏感信息仅存储在网络设备14的易失性存储器上。为了实现本公开的技术，网络设备14执行非接触式供应操作以在网络设备14的每个引导周期期间取回导引信息。网络设备14处理导引信息以确定网络设备14的第一初始化是否已经发生。如果第一初始化还没有发生，则网络设备14通过将其自身配置为将文件系统的至少一部分挂载到网络设备的易失性存储器而不是网络设备的非易失性存储器来执行第一初始化并重新引导其本身。

[0028] 对于每个后续引导周期，网络设备14将文件系统的至少一部分挂载到易失性存储器和/或加密非易失性存储器的至少一部分，诸如例如非易失性存储器的交换部分。此外，网络设备14执行另一个非接触式供应操作以请求导引信息。网络设备14处理导引信息以确定第一初始化是否已经发生。响应于确定第一初始化已经发生，网络设备14执行自举操作。作为自举操作的示例，网络设备可以将其自身配置用于由另一网络设备进行远程管理，诸如通过获得用于远程网络设备的IP地址或用于认证协调器服务器20的安全凭证，或者通过建立本地管理员帐户，协调器服务器20可以使用该帐户登录网络设备14，等。

[0029] 在以下算法中阐述了根据本公开的技术的示例操作：

[0030] #检查是否第一次运行

[0031] 如果(if)[第一次运行]；则

[0032] 做第一初始化：

[0033] -设置非易失性配置(例如禁用控制台端口或设置根密码)。

[0034] -下载并安装包含rc脚本的包，以便将基于存储器的主文件系统(MFS)初始化到具有加密交换、挂载文件系统和初始化文件系统的易失性存储器，从而使得MFS在引导时挂载到易失性存储器。

[0035] -重新启动网络设备(这会重新启动网络设备以及安全的非接触式供应过程)

[0036] 否则

[0037] 根据用户的判断，进行正常的配置操作

[0038] -此处执行的动作，取决于它们是什么，可能会或可能不会在断电后继续存在，取决于动作是否会影响被移动到易失性存储器中的MFS的文件系统中的文件。

[0039] fi

[0040] 在本公开的技术的一个示例中，在启动时，网络设备14执行第一非接触式供应操作21以从DHCP服务器16请求用于自举服务器18的地址信息。通常，网络设备14使用不安全的协议来进行该请求，并盲目地信任响应。在一些示例中，地址信息是网络设备14可以从其获得配置信息的一个或多个自举服务器18的列表。在一些示例中，列表是元组数据结构，其指定每个自举服务器18的主机名和端口。地址信息是重定向信息，其将配置信息的请求从网络设备14重定向到自举服务器18。

[0041] 在接收到用于自举服务器18的地址信息时，网络设备14执行第二非接触式供应操作23以从自举服务器18请求用于网络设备14的导引信息。在一些示例中，网络设备14使用

不安全的连接来进行请求。网络设备14可以盲目地信任自举服务器18的TLS证书。自举服务器18可以经由诸如IDevID的TLS级客户端证书来认证网络设备14。网络设备14从自举服务器18接收导引信息。通常，从自举服务器18接收的配置信息被签名。

[0042] 网络设备14验证配置信息中的自举服务器18的签名。在验证签名之后，网络设备14处理导引信息以确定网络设备的第一初始化是否已经发生。如果第一初始化还没有发生，则网络设备14执行第一初始化。例如网络设备14可以通过配置本地用户访问许可来限制本地用户访问并将其自身配置为将文件系统的至少一部分挂载到网络设备14的易失性存储器而不是网络设备14的非易失性存储器来执行第一初始化。此外，网络设备14重新启动自身。

[0043] 导引信息可以包括用于执行本地用户访问许可的配置的指令。例如网络设备14可以通过执行网络设备14的安全加固来基于导引信息配置本地用户访问许可，以限制本地用户对网络设备14的访问。例如网络设备14可以禁用一个或者更多的控制台端口和/或网络设备14的开放管理端口，或者将根访问密码设置到网络设备14。通常，网络设备14将本地用户访问许可存储在网络设备14的非易失性存储器中，使得在对本地当网络设备14断电时，用户访问许可不会丢失。

[0044] 在一些示例中，导引信息指定网络设备14将使用的特定引导映像、网络设备14应当使用的初始配置、以及用于由网络设备14执行的一个或多个脚本。在一些示例中，导引信息指定特定的操作系统类型和版本。在一些示例中，网络设备14使用导引信息来配置一个或多个远程管理协议，诸如通过SSH的NETCONF，以及配置网络设备14是否发起出站SSH连接，或者打开启用进入SSH连接的端口。在一些示例中，网络设备14使用导引信息来配置协调器服务器20或另一用户是否可以经由根或其他登录来访问网络设备14。在一些示例中，网络设备14使用导引信息来配置可以如何执行SSH认证(例如经由密码、公钥加密、RADIUS、tacplus等)。

[0045] 对于每个后续引导周期，网络设备14将文件系统的至少一部分挂载到易失性存储器和/或加密非易失性存储器的至少一部分。此外，网络设备14执行第三非接触式供应操作25以请求导引信息。网络设备14处理导引信息以确定网络设备14的第一初始化是否已经发生。响应于确定第一初始化已经发生，网络设备14执行自举操作。作为自举操作的示例，网络设备14可以将其自身配置为由另一网络设备(例如协调器服务器20)进行远程管理。此外，网络设备14可以执行网络设备14的易失性配置。作为易失性配置的示例，网络设备14可以禁用系统端口上的控制台，启用经由SSH对系统服务的访问，禁用经由SSH对网络设备14的密码的使用，允许经由SSH进行根登录，为SSH公钥认证配置根帐户，并配置网络设备14以启动出站SSH会话。这些配置可能在网络设备14断电或重新启动时丢失。在完成自举操作之后，网络设备14可以建立到协调器服务器20的安全管理连接(例如NETCONF)。此外，网络设备14开始正常操作。例如在网络设备14是路由器的情况下，网络设备14可以开始网络业务31的处理和路由。

[0046] 通常，所有控制平面和管理业务都被加密。虽然安全的零触摸供应(例如安全的ZTP)和SSH上的NETCONF建立在安全传输层之上，但并非所有协议都是这样(例如syslog)。因此，作为自举过程的一个方面，VPN可以被配置在网络设备14和自举服务器18之间。可以使用不同的技术来实现这些VPN。例如它们可以用软件或硬件实现。在一个示例中，MS-MPC

线卡可以用于执行所有控制平面和管理平面业务的硬件加密。在一些示例中，本文描述的安全非接触式供应操作可以用于配置MS-MPC线卡。在其他示例中，用户通过经由网络设备14或协调器服务器20的访问将MS-MPC线卡配置为通过管理连接(例如通过SSH的NETCONF)发生的交互步骤。

[0047] 在一些示例中，自举过程可以进一步分为两个操作：第一个是网络设备14配置有导引信息的操作，第二个是在协调器服务器20第一次建立到网络设备14的连接之后，协调器服务器20或另一网络管理系统利用附加软件应用来配置网络设备14的操作。在一些示例中，每个非接触式供应操作以网络设备14向自举服务器18发送“自举完成”进度报告而结束。自举服务器18可以将该报告传播到协调器服务器20，从而提供用于何时协调器服务器20可以在网络设备14上执行第一次操作的信号。

[0048] 在一些示例中，协调器服务器20可以从服务提供商网络32的凭证服务器10获得所有权凭证33。例如凭证服务器10可以提供认证运营商证书的基于REST的API。凭证服务器10验证客户网络30内的诸如网络设备14的设备由客户网络30的运营商拥有。凭证服务器10将协调器服务器20的所有者证书编码到所有权凭证中；网络设备14可以使用所有者证书来验证由所有者在非接触式供应操作期间签署的导引信息。例如网络设备14可以使用预先配置的信任锚来验证所有权凭证是由可信机构生成的。网络设备14还可以例如检查所有权凭证以确保其包含网络设备的序列号，并因此知道所有权凭证应用于网络设备14。凭证服务器10可以将由网络设备14的制造商(或制造商本身)信任的签名机构签名的凭证发给访问客户网络30的每个授权设备。

[0049] 作为一个示例，协调器20为所有者证书生成PKI。协调器20从凭证服务器10请求以提供针被授权访问客户网络30的设备列表(由其序列号标识)的、包含所提供的域证书的凭证。凭证服务器10提供授权访问客户网络30的设备的所有权凭证列表。为了后续使用，协调器20存储设备特定的所有权凭证和所有者证书。协调器20可以使用所存储的设备特定的所有权凭证和所有者证书来在非接触式供应操作期间为网络设备14签署自举数据以配置如上所述的网络设备。

[0050] 因此，通过使用本公开的技术，网络设备可以将在自举过程期间获得的配置信息保持在网络设备的易失性存储器内。在断开对网络设备的电源时，网络设备丢失可能对具有对网络设备的物理访问的恶意行为者有用的任意信息，诸如用户数据、配置信息或引导映像。每个引导周期，网络设备14可以在启动时使用非接触式供应操作来取回新的导引信息。此外，在第一初始化之后，禁用诸如经由控制台端口对网络设备14的本地访问。

[0051] 因此，本公开的技术提供了对计算机相关的网络设备部署和配置领域的具体改进。例如本公开的技术可以允许部署到网络设备的公共空间，该网络设备被保护免于恶意行为者的物理或本地攻击。此外，本公开的技术可以允许非接触式供应的使用来安全地和远程地配置网络设备。另外，本公开的技术可以降低最终用户部署和配置网络设备以在企业网络内操作的成本和技术负担。此外，本公开的技术可以降低网络设备的部署、维护和升级的复杂性。

[0052] 图2是示出了根据本公开的技术的示例网络设备200的框图。在一些示例中。网络设备200是图1的网络设备14的示例。例如网络设备200可以对应于路由器、网桥、集线器、交换机、服务器、打印机、网关、防火墙、IDP设备、或其他网络设备。在图2的示例中，网络设备

200包括用户接口模块202、控制单元208和网络接口220。

[0053] 用户接口202被配置为向/从诸如网络管理员的用户发送/接收数据。通常，用户界面202包括控制台端口，其允许诸如管理员的用户进行本地访问。然而，在一些示例中，用户接口202是或以其他方式包括工作站、键盘、指示设备、语音响应系统、视频相机、生物识别检测/响应系统、按钮、传感器、移动设备、控制板、麦克风、存在敏感屏幕、网络或用于检测来自人或机器的输入的任意其他类型的设备。在一些示例中，用户接口202还包括用于向用户显示输出的显示器。显示器可以用作使用包括以下技术的输出设备：液晶显示器(LCD)、量子点显示器、点阵显示器、发光二极管(LED)显示器、有机发光二极管(OLED)显示器、阴极射线管(CRT)显示器、电子墨水或单色、彩色或能够生成触觉、音频和/或视觉输出的任意其他类型的显示器。在其他示例中，用户接口202可以以另一种方式向用户产生输出，诸如经由声卡、视频图形适配器卡、扬声器、存在敏感屏幕、一个或多个USB接口、视频和/或音频输出接口、或能够生成触觉、音频、视频或其他输出的任意其他类型的设备。在一些示例中，用户接202可以包括存在敏感显示器，其可以用作用户界面设备，用户界面设备操作为一个或多个输入设备和一个或多个输出设备两者。

[0054] 控制单元208包括用于执行本公开的技术的硬件。处理器204可以包括微处理器、控制器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或等效的分立或集成逻辑电路中的任意一个或多个。网络设备还包括非易失性存储器230和易失性存储器240。如本文所述，“非易失性存储器”指的是即使对非易失性存储器的供电丢失也保留数据的存储设备。相反，如本文所述，“易失性存储器”指的是如果丢失了对易失性存储器的供电则丢失数据的存储设备。替代地，控制单元208可以包括专用硬件，诸如一个或多个集成电路、一个或多个专用集成电路(ASIC)、一个或多个专用特殊处理器(ASSP)、一个或多个现场可编程门阵列(FPGA)、或者用于执行本文描述的技术的专用硬件的前述示例的任意组合。

[0055] 非易失性存储器230可以包括磁盘驱动器、光盘驱动器、存储器，例如随机存取存储器(RAM)、只读存储器(ROM)、可编程只读存储器(PROM)、可擦除可编程只读存储器(EPROM)、电子可擦除可编程只读存储器(EEPROM)、闪存等，包括用于使处理器204执行归因于它们的动作的可执行指令。

[0056] 易失性存储器100可以包括存储器，诸如随机存取存储器(RAM)或闪存等，包括用于使处理器204执行归因于它们的动作的可执行指令。

[0057] 在图2的示例中，控制单元208包括设备模块212和协议214，其可以包括由控制单元208或控制单元208的离散的独立硬件单元执行的软件模块。当设备模块212时协议214中的任意一个或所有包括软件时，可由处理器执行的用于设备模块212和协议214的指令可以被编码在网络设备200的计算机可读介质中，诸如非易失性存储器230或易失性存储器240。

[0058] 网络接口220可以包括用于连接到计算机网络的设备的任意接口，该设备诸如图1的DHCP服务器16、自举服务器18或协调器服务器20。例如网络接口220可以包括以太网接口、千兆以太网接口、电话调制解调器、电缆调制解调器、卫星调制解调器或其他网络接口。在一些示例中，网络接口220包括一个或多个网络接口卡。

[0059] 设备模块212通常对应于网络设备200特有的组件。例如当网络设备200包括路由器时，设备模块212可以包括维护路由信息库的控制平面、维护转发信息库的转发引擎、一

个或多个路由协议、或通过网络路由分组所需的其他模块。作为另一示例，当网络设备200包括安全设备时，设备模块212可以包括协议解码器模块、应用识别模块和攻击检测模块、或其他网络安全模块。协议214包括用于与管理设备10和/或其他网络设备通信的一个或多个通信协议。例如协议214可以包括非接触式供应协议，诸如ZTP 216。协议214还可以包括一个或多个路由协议、安全协议或其他协议，这取决于网络设备200对应的设备的类型。

[0060] 根据本公开的技术，网络设备200执行安全的远程自举操作。在启动时，处理器204执行第一非接触式供应操作以从DHCP服务器16请求针对自举服务器18的地址信息。在接收到针对自举服务器18的地址信息时，处理器204执行第二非接触式供应操作以从自举服务器18请求用于网络设备200的导引信息。

[0061] 处理器204处理导引信息以确定网络设备200的第一初始化是否已经发生。如果第一初始化还没有发生，则处理器204执行第一初始化。例如处理器204可以通过配置网络设备200的本地用户访问许可270并配置网络设备200以将文件系统250的至少一部分挂载到易失性存储器240而不是非易失性存储器230来执行第一初始化。进一步地，处理器204使网络设备200重新启动。

[0062] 为了配置本地用户访问许可270，处理器204可以通过禁用网络设备200的一个或多个控制台端口和/或开放管理端口或者通过将根访问密码设置到网络设备200来执行网络设备200的安全加固。通常，处理器204将本地用户访问许可270存储在非易失性存储器230中，使得本地用户访问许可270在网络设备200断电时不会丢失。

[0063] 对于每个后续引导周期，处理器204执行操作系统级初始化。例如处理器204将文件系统250的至少一部分挂载到易失性存储器240。作为另一个示例，处理器204加密非易失性存储器230的至少一部分，诸如交换部分260。此外，处理器204执行非接触式供应级初始化。作为示例，处理器204执行非接触式供应操作以从自举服务器18取回导引信息。处理器204将导引信息存储在易失性存储器240中，使得在失去对网络设备200的供电或重新启动时不保留导引信息。处理器204处理导引信息以确定网络设备200的第一初始化是否已经发生。响应于确定第一初始化已经发生，处理器204执行自举操作。作为自举操作的示例，处理器204可以将网络设备200配置为由另一网络设备(例如协调器服务器20)进行远程管理。例如处理器204可以分配用于与协调器服务器20通信的主机名、IP地址或端口，处理器204可以定义信任锚证书以对协调器服务器20进行认证，并且处理器204可以建立管理员帐户，协调器服务器20可以用管理员帐户来访问网络设备200。作为进一步的示例，处理器204可以禁用系统端口上的控制台，启用经由SSH对系统服务的访问，禁用经由SSH对网络设备200的密码的使用，允许经由SSH进行根登录，配置根帐户用于SSH公钥认证，并配置网络设备200以启动出站SSH会话(例如使用协调器20)。通常，处理器204存储在该阶段(例如在第一初始化已经发生之后)在易失性存储器240中执行的任意配置，使得在网络设备200断电或重新启动时不保留配置。在完成自举操作之后，处理器204可以建立到协调器服务器20的安全管理连接(例如NETCONF)并开始网络设备200的操作。例如在网络设备200是路由器的情况下，处理器204可以开始网络业务的处理和路由。

[0064] 因此，通过使用本公开的技术，网络设备200可以将文件系统250的至少一部分保持在易失性存储器240内。在网络设备200断电源时，易失性存储器240丢失文件系统250的一部分。然后，网络设备200可能丢失用于访问加密交换260的加密密码。因此，网络设备200

不保留文件系统250或交换260中的任意信息，这些信息可能对具有对网络设备200的物理访问的恶意行为者有用。每个引导周期中，网络设备200可以执行新的非接触式供应操作以执行网络设备200的自举，并且因此将文件系统250的一部分重新挂载到易失性存储器240。此外，在第一初始化之后，禁用例如经由用户界面202的控制台端口来对网络设备200的本地访问。

[0065] 图3是示出了根据本公开的技术的示例服务器300的框图。服务器300是可以实现例如图1的DHCP服务器16、自举服务器18、协调器服务器20或凭证服务器10中的一个或多个的计算设备。在图3的示例中，服务器300包括用户接口302、控制单元308和网络接口320。

[0066] 用户接口302被配置为向/从诸如网络管理员的用户发送/接收数据。在一些示例中，用户接口302是或以其他方式包括工作站，键盘，指示设备，语音响应系统，视频相机，生物识别检测/响应系统，按钮，传感器，移动设备，控制板，麦克风，存在敏感屏幕，网络或用于检测来自人或机器的输入的任意其他类型的设备。在一些示例中，用户接口302还包括用于向用户显示输出的显示器。显示器可以用作使用包括以下各项的技术的输出设备：液晶显示器(LCD)、量子点显示器、点阵显示器、发光二极管(LED)显示器、有机发光二极管(OLED)显示器、阴极射线管(CRT)显示器、电子墨水或单色、彩色或能够生成触觉、音频和/或视觉输出的任意其他类型的显示器。在其他示例中，用户接口302可以以另一种方式向用户产生输出，诸如经由声卡、视频图形适配器卡、扬声器、存在敏感屏幕、一个或多个USB接口、视频和/或音频输出接口、或能够生成触觉、音频、视频或其他输出的任意其他类型的设备。在一些示例中，用户接口302可以包括存在敏感显示器，其可以用作用户接口设备，用户接口设备操作一个或多个输入设备和一个或多个输出设备两者。

[0067] 网络接口320可以包括用于连接到计算机网络的设备的任意接口，诸如客户网络30的网络设备14。例如网络接口320可以包括以太网接口、千兆以太网接口、电话调制解调器、电缆调制解调器、卫星调制解调器或其他网络接口。在一些示例中，网络接口320包括一个或多个网络接口卡。

[0068] 控制单元308包括用于执行本公开的技术的硬件。处理器304可以包括微处理器、控制器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或等效的分立或集成逻辑电路中的任意一个或多个。存储设备306可以包括磁盘驱动器、光盘驱动器、存储器、例如随机存取存储器(RAM)、只读存储器(ROM)、可编程只读存储器(PROM)、可擦除可编程只读存储器(EPROM)、电子地可擦除可编程只读存储器(EEPROM)、闪存，包括用于使处理器304执行归因于它们的动作的可执行指令。替代地，控制单元308可以包括专用硬件，诸如一个或多个集成电路、一个或多个专用集成电路(ASIC)、一个或多个专用特殊处理器(ASSP)、一个或多个现场可编程门阵列(FPGA)、或者用于执行本文描述的技术的专用硬件的前述示例的任意组合。

[0069] 在图3的示例中，控制单元308包括设备管理器310、设备模块312和协议314，其可以包括由控制单元308或控制单元308的离散的独立硬件单元执行的软件模块。当设备管理器310、设备模块312和协议314中的任意一个或者所有包括软件，例如可执行软件模块时，针对设备管理器310、设备模块312和协议314的由处理器执行的指令可以被编码在诸如存储设备306的计算机可读介质中。

[0070] 设备管理器310与例如网络设备14的一个或多个被管理设备交互以管理网络设

备。在一个示例中，设备管理器310执行NETCONF的实现。设备管理器310经由网络接口320向被管理网络设备14发送电信号。因此，设备管理器310向例如网络设备14发送和接收分组，分组包括用于经由诸如因特网的网络间接地管理被管理网络设备14的数据。

[0071] 设备模块312通常对应于服务器300特有的组件。例如设备模块312可以包括维护路由信息库的控制平面、维护转发信息库的转发引擎、一个或多个路由协议、或者通过网络路由分组所需的其他模块。

[0072] 在服务器300是图1的DHCP服务器16的示例中，设备模块312包括用于向客户网络30内的设备提供DHCP服务的DHCP模块，诸如网络设备14、自举服务器18和客户设备36。在一些示例中，服务器300可以响应于网络设备14的非接触式供应操作来提供重定向信息。例如响应于第一非接触式供应操作，其中网络设备14请求网络分配并请求导引信息的重定向信息，服务器300提供用于到达自举服务器18的地址信息。通常，服务器300使用不安全的协议提供该信息。在一些示例中，地址信息是网络设备14可以从其获得配置信息的一个或多个自举服务器18的列表。在一些示例中，列表是元组数据结构，其指定用于自举服务器18的主机名和端口。在一些示例中，地址信息是重定向信息，其将对配置信息的请求从网络设备14重定向到自举服务器18。

[0073] 在服务器300是图1的自举服务器18的示例的示例中，服务器300可以用作网络设备14的导引信息的源。如本文所述，网络设备14可以经由非接触式供应操作从自举服务器18请求导引信息以执行网络设备14的自动配置。在一些示例中，非接触供应操作是ZTP操作。例如响应于来自网络设备14的第二非接触式供应请求，服务器300为网络设备14提供导引信息。在一些示例中，导引信息指定网络设备14将使用的特定启动映像，网络设备14应该使用的初始配置，以及用于由网络设备14执行的一个或多个脚本。在一些示例中，导引信息指定特定的操作系统类型和版本。在一些示例中，网络设备14使用导引信息来配置一个或多个远程管理协议，诸如通过SSH的NETCONF，以及配置网络设备14是否发起出站SSH连接，或者打开启用入站SSH连接的端口。在一些示例中，网络设备14使用导引信息来配置协调器服务器20或另一用户是否可以经由根或其他登录来访问网络设备14。在一些示例中，网络设备14使用导引信息来配置SSH认证可以如何被执行(例如经由密码、公钥加密、RADIUS、tacplus等)。

[0074] 在服务器300是图1的协调器服务器20的示例的示例中，服务器300可以从服务提供商网络32的凭证服务器10获得所有权凭证，向DHCP服务器16提供DHCP配置以使DHCP服务器16能够向客户网络30内的设备提供DHCP服务，或者向自举服务器18提供自举配置信息以使自举服务器18能够向网络设备14提供自举服务。另外，一旦网络设备14被部署并激活，服务器300就可以建立安全管理连接使用诸如NETCONF的通信协议来管理网络设备14。此外，协调器服务器20可以将网络业务转发到网络设备14以进行处理和路由。

[0075] 在示例中，其中服务器300是图1的凭证服务器10的示例，服务器300可以提供认证运营商证书的基于REST的API。例如服务器300验证客户网络30内的诸如网络设备14的设备由客户网络30的运营商拥有。服务器300将协调器服务器20的所有者证书编码到所有权凭证中；网络设备14可以使用所有者证书来验证由所有者在非接触式供应操作期间签名的导引信息。服务器300可以将由网络设备14的制造商(或制造商自身)信任的签名机构签名的凭证发布给访问客户网络30的每个授权设备。

[0076] 协议314包括用于通过网络进行通信的一个或多个网络通信协议。例如协议314可以包括一个或多个路由协议、安全协议或其他协议，例如诸如ZTP 316、DHCP 318的非接触式供应协议，或用于通过未在图3中明确描绘的网络进行通信的其他网络协议，诸如SSH、PPP、PPPoE、PPPoA、MPLS、BGP、SNMP、NETCONF等。

[0077] 图4是示出了根据本发明的技术的示例性安全远程自举操作的流程图。为方便起见，参照图1描述图4。

[0078] 在一个示例中，在启动时，网络设备14执行第一非接触式供应操作以从DHCP服务器16请求针对自举服务器18的地址信息(404)。作为响应，DHCP服务器16提供地址信息作为一个或多个自举服务器18的列表，网络设备14可以从其中获取配置信息(406)。在一些示例中，列表是元组数据结构，其指定针对自举服务器18的主机名和端口。在一些示例中，地址信息是重定向信息，其将对配置信息的请求从网络设备14重定向到自举服务器18。

[0079] 在接收到针对自举服务器18的地址信息时，网络设备14执行第二非接触式供应操作23以从自举服务器18请求用于网络设备14的导引信息(408)。自举服务器18将引导配置信息提供给网络设备14(410)。网络设备14从自举服务器18接收导引信息。通常，从自举服务器18接收的配置信息被签名。

[0080] 网络设备14处理导引信息以确定网络设备的第一初始化是否已经发生。响应于确定第一初始化还没有发生，网络设备14执行第一初始化(412)。例如网络设备14可以通过配置本地用户访问许可并将其自身配置为将文件系统的至少一部分挂载到网络设备14的易失性存储器而不是网络设备14的非易失性存储器来执行第一初始化。例如网络设备14可以通过禁用网络设备14的一个或多个控制台端口和/或开放管理端口或者通过设置到网络设备14的根访问密码来执行网络设备14的安全加固。通常，网络设备14将本地用户访问许可存储在网络设备14的非易失性存储器中，使得本地用户访问许可在网络设备14断电时不会丢失。此外，网络设备14重新启动自身。

[0081] 对于每个后续引导周期，网络设备14将文件系统的至少一部分挂载到易失性存储器。在一些示例中，网络设备14加密非易失性存储器的至少一部分，诸如文件系统的交换部分。此外，网络设备14执行第三非接触式供应操作以请求导引信息(414)。网络设备14处理导引信息以确定网络设备14的第一初始化是否已经发生。响应于确定第一初始化已经发生，网络设备14执行自举操作(418)。作为自举操作的示例，网络设备14将其自身配置为由另一网络设备(例如协调器服务器20)进行远程管理。此外，网络设备14可以执行网络设备14的易失性配置。作为易失性配置的示例，网络设备14可以禁用系统端口上的控制台，启用经由SSH对系统服务的访问，禁用经由SSH对网络设备14的密码的使用，允许经由SSH的根登录，针对SSH公钥认证配置根帐户，并配置网络设备14以启动出站SSH会话。

[0082] 在完成自举操作之后，协调器服务器20和网络设备14可以彼此建立安全管理连接(例如NETCONF)(420)。此外，网络设备14开始正常操作(422)。例如在网络设备14是路由器的情况下，网络设备14开始网络业务31的处理和路由。

[0083] 本公开中描述的技术可至少部分地以硬件、软件、固件或其任意组合来实现。例如所描述的技术的各个方面可以在一个或多个处理器内实现，一个或多个处理器包括一个或多个微处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或任意其他等效的集成或离散逻辑电路、以及这些组件的任意组合。术语“处理器”或“处理电

路”通常可以指任意前述逻辑电路，单独或与其他逻辑电路组合，或任意其他等效电路。包括硬件的控制单元还可以执行本公开的一种或多种技术。

[0084] 这样的硬件、软件和固件可以在相同设备内或在单独的设备内实现，以支持本公开中描述的各种操作和功能。另外，所描述的单元、模块或组件中的任意一个可以一起实现或单独实现为离散但可互操作的逻辑设备。将不同特征描述为模块或单元旨在突出不同的功能方面，并且不一定暗示这些模块或单元必须由单独的硬件或软件组件实现。相反，与一个或多个模块或单元相关联的功能可以由单独的硬件或软件组件执行，或者集成在公共或单独的硬件或软件组件中。

[0085] 本公开中所描述的技术还可在包含指令的诸如计算机可读存储介质的计算机可读介质中体现或编码。嵌入或编码在计算机可读存储介质中的指令可以使可编程处理器或其他处理器例如当执行指令时执行该方法。计算机可读存储介质可包括随机存取存储器(RAM)、只读存储器(ROM)、可编程只读存储器(PROM)、可擦除可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM)、闪存、硬盘、CD-ROM、软盘、盒式磁带、磁性介质、光学介质或其他计算机可读介质。

[0086] 除上述之外或作为上述替代，描述了以下实施例。以下示例的任意一个中描述的特征可以与本文描述的其他示例中的任意一个一起使用。

[0087] 示例1.一种方法，包括：由网络设备的一个或多个处理器执行针对网络设备的导引信息的第一请求；所述一个或多个处理器处理所述导引信息，以确定所述网络设备的第一初始化还没有发生；响应于确定网络设备的第一初始化还没有发生，通过以下各项执行第一初始化：由一个或多个处理器并使用导引信息，配置网络设备以将文件系统的至少一部分挂载到网络设备的易失性存储器，而不是网络设备的非易失性存储器；并且由一个或多个处理器重新启动网络设备；在重新启动网络设备之后：由一个或多个处理器执行针对网络设备的导引信息的第二请求；由所述一个或多个处理器处理所述导引信息，以确定所述网络设备的第一初始化已经发生；并且响应于确定网络设备的第一初始化已经发生，由一个或多个处理器执行网络设备的自举操作。

[0088] 示例2.示例1的方法，还包括在重新启动网络设备之后将文件系统的至少一部分挂载到网络设备的易失性存储器。

[0089] 示例3.示例2的方法，还包括：在将文件系统的至少一部分安装到网络设备的易失性存储器之后，当网络设备断电时，从网络设备的易失性存储器中失去文件系统的至少一部分。

[0090] 示例4.示例1至4中任一组合的方法，其中执行网络设备的自举操作包括配置网络设备以用于由第二网络设备进行远程管理。

[0091] 示例5.示例4的方法，其中配置所述网络设备以用于由所述第二网络设备进行远程管理包括处理所述导引信息以获得主机名、网络地址、端口、网络协议、或者所述第二网络设备的安全证书中的一个或多个。

[0092] 示例6.示例4至5的任意组合的方法，其中配置网络设备以用于由第二网络设备进行远程管理包括由网络设备并基于导引信息初始化与第二个网络设备的远程通信会话。

[0093] 示例7.如示例1至6中任一组合的方法，其中执行网络设备的自举操作包括用一次性密钥加密网络设备的非易失性存储器的交换空间。

[0094] 示例8.示例1至7中任一组合的方法,其中所述网络设备是第一网络设备,其中执行针对所述网络设备的所述导引信息的所述第一请求包括:经由第一非接触式供应操作从一个或多个网络设备请求所述第一网络设备的所述导引信息,以及其中执行针对所述网络设备的所述导引信息的所述第二请求包括:经由第二非接触式供应操作从所述一个或多个网络设备请求所述第一网络设备的所述导引信息。

[0095] 示例9.示例8的方法,其中第一和第二非接触式供应操作是第一零接触供应(ZTP)操作和第二零接触供应(ZTP)操作。

[0096] 示例10.示例8至9的任意组合的方法,还包括:在经由所述第一非接触式供应操作来请求针对所述第一网络设备的所述导引信息之前,由所述一个或多个处理器从动态主机配置协议(DHCP)服务器,并且经由第三非接触式供应操作,请求针对所述一个或多个网络设备的地址信息。

[0097] 示例11.示例1至10中任一组合的方法,其中执行第一初始化还包括由一个或多个处理器配置对网络设备的本地用户访问许可。

[0098] 示例12.示例11所述的方法,其中配置对所述网络设备的所述本地用户访问许可包括以下至少一项:由所述一个或多个处理器禁用所述网络设备的一个或多个控制台端口;或者由所述一个或多个处理器设置用于对所述网络设备进行根访问的密码。

[0099] 示例13.示例11至12的任意组合的方法,其中配置对所述网络设备的所述本地用户访问许可还包括将对所述网络设备的所述本地用户访问许可存储在所述网络设备的所述非易失性存储器中而不是所述网络设备的所述易失性存储器中。

[0100] 示例14.一种网络设备,包括:非易失性存储器;易失性存储器;以及一个或多个处理器,被配置为:执行针对所述网络设备的导引信息的第一请求;处理所述导引信息以确定所述网络设备的第一初始化还没有发生;响应于确定所述网络设备的所述第一初始化还没有发生,通过以下各项执行所述第一初始化:利用所述导引信息配置所述网络设备以将文件系统的至少一部分挂载到所述易失性存储器而不是所述非易失性存储器;以及重新启动所述网络设备;在重新启动所述网络设备后:执行针对所述网络设备的所述导引信息的第二次请求;处理所述导引信息以确定所述网络设备的所述第一初始化已经发生;以及响应于确定所述网络设备的所述第一初始化已经发生,执行所述网络设备的自举操作。

[0101] 示例15.示例14所述的网络设备,其中所述一个或多个处理器还被配置为在重新启动所述网络设备之后将所述文件系统的至少一部分挂载到所述网络设备的易失性存储器。

[0102] 示例16.示例15的网络设备,其中在将文件系统的至少一部分挂载到网络设备的易失性存储器之后,网络设备还被配置为在网络设备断电源时,从易失性存储器中丢失文件系统的至少一部分。

[0103] 示例17.示例14至16的任意组合的网络设备,其中为了执行网络设备的自举操作,所述一个或多个处理器还被配置为将网络设备配置为由第二网络设备进行远程管理。

[0104] 示例18.示例14至17的任意组合的网络设备,其中为了执行网络设备的自举操作,所述一个或多个处理器还被配置为用一次性密钥加密网络设备的非易失性存储器的交换空间。

[0105] 示例19.示例14至18的任意组合的网络设备,其中所述网络设备是第一网络设备,

其中为了执行针对所述网络设备的所述导引信息的第一请求，所述一个或多个处理器是被配置为经由第一非接触式供应操作从一个或多个网络设备请求针对第一网络设备的导引信息，并且其中为了执行针对网络设备的导引信息的第二请求，一个或多个处理器被配置为经由第二非接触式供应操作从一个或多个网络设备请求针对第一网络设备的导引信息。

[0106] 示例20.一种非暂时性计算机可读介质，包括指令，该指令被配置为使网络设备的一个或多个处理器用于：执行针对网络设备的导引信息的第一请求；处理导引信息以确定网络设备的第一初始化还没有发生；响应于确定网络设备的第一初始化还没有发生，通过以下各项执行第一初始化：利用导引信息来配置网络设备以将文件系统的至少一部分挂载到网络设备的易失性存储器中而不是网络设备的非易失性存储器；并重新启动网络设备；在重新启动网络设备后：执行针对网络设备的导引信息的第二次请求；处理导引信息以确定网络设备的第一初始化已经发生；并且响应于确定网络设备的第一初始化已经发生，执行网络设备的自举操作。

[0107] 此外，可以将上述任意示例中阐述的任意具体特征组合成所描述技术的有益示例。也就是说，任意特定特征通常适用于本发明的所有示例。已经描述了本发明的各种示例。

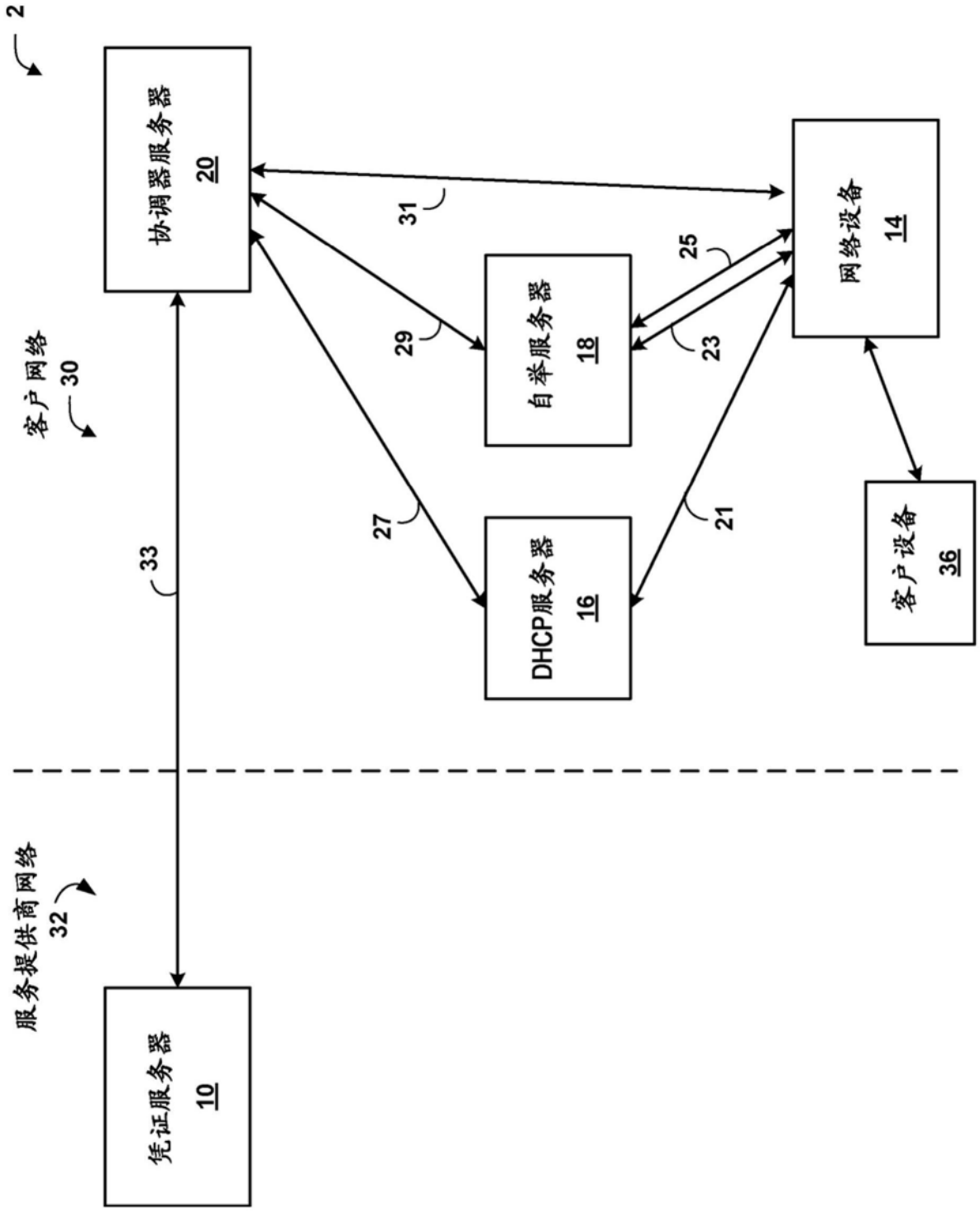

2
协调器服务器
20
网络设备
14
31
25
自举服务器
18
29
23
客户网络
30
27
21
DHCP服务器
16
客户设备
36
33
服务提供商网络
32
凭证服务器
10

图1

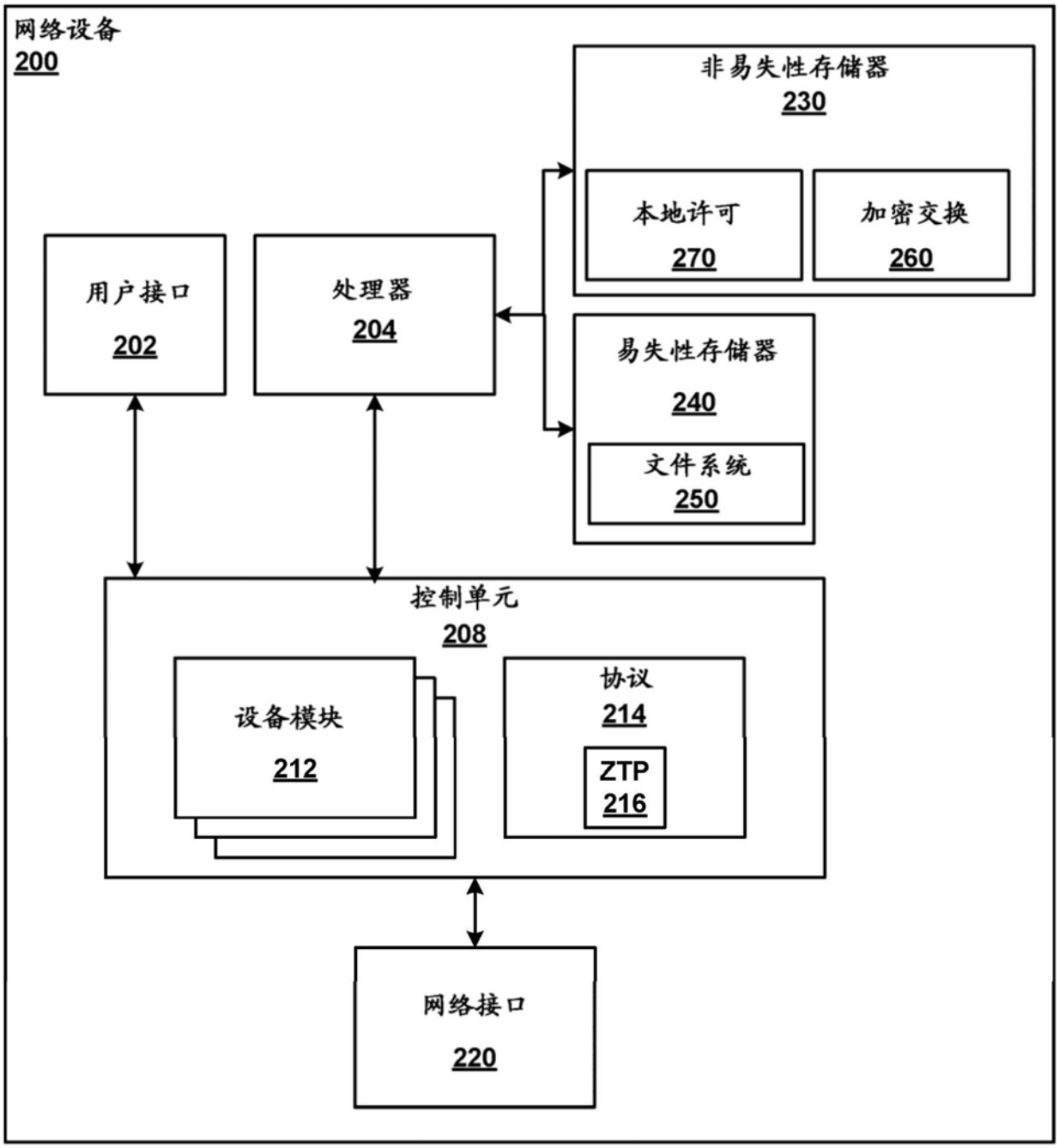

网络设备
200
非易失性存储器
230
本地许可
270
加密交换
260
用户接口
202
处理器
204
易失性存储器
240
文件系统
250
控制单元
208
设备模块
212
协议
214
ZTP
216
网络接口
220

图2

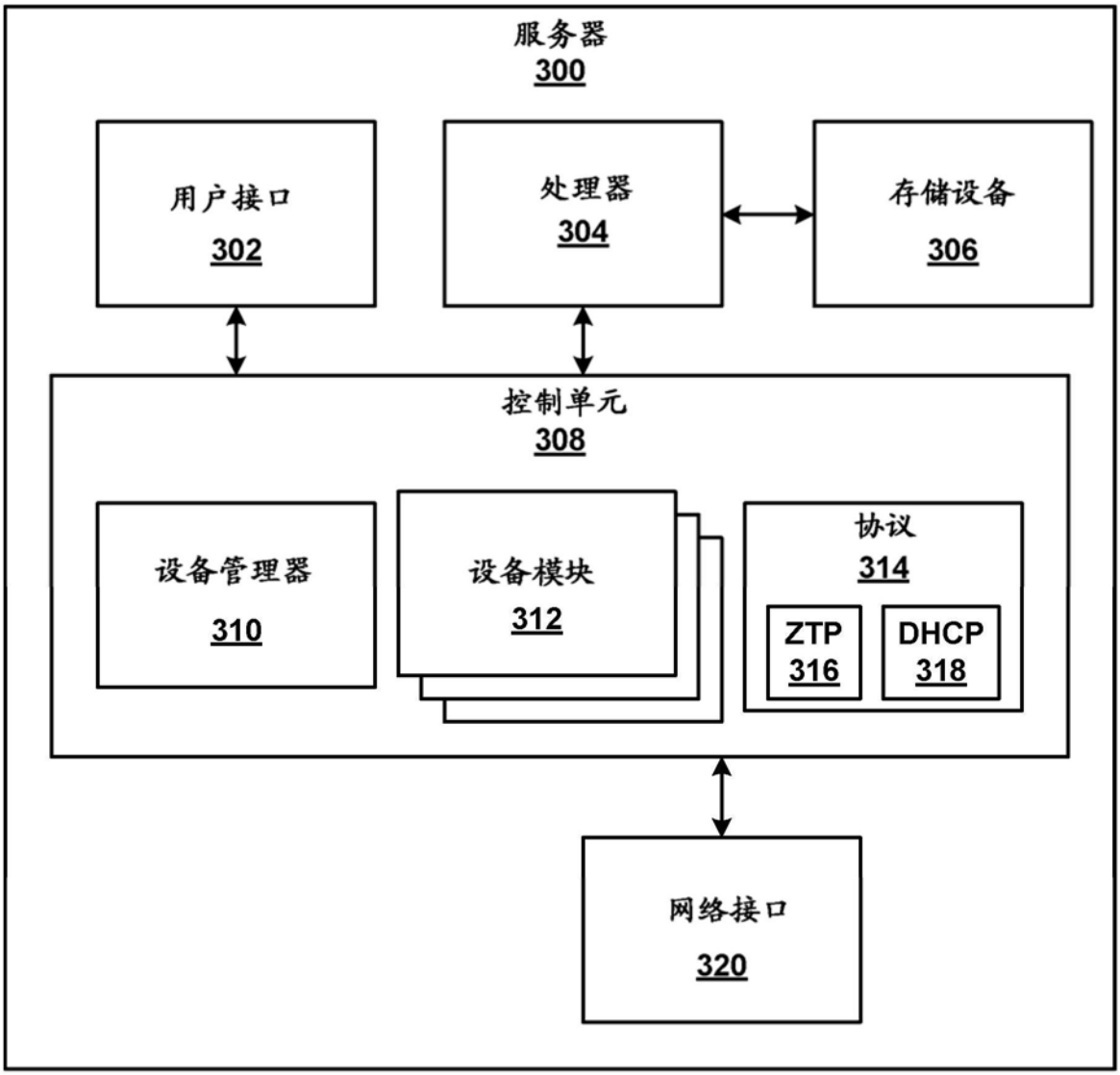

服务器
300
用户接口
302
处理器
304
存储设备
306
控制单元
308
设备管理器
310
设备模块
312
协议
314
ZTP
316
DHCP
318
网络接口
320

图3

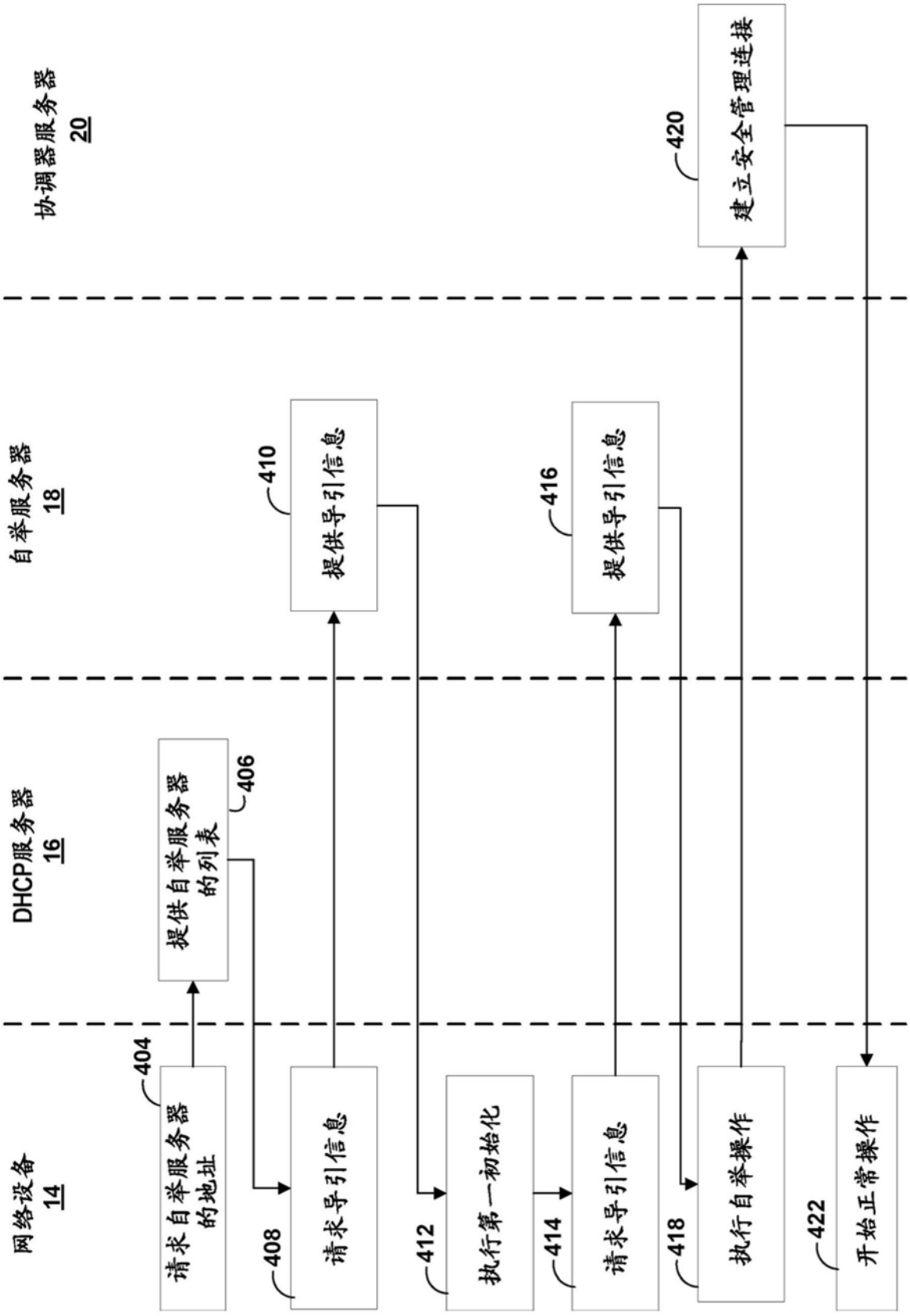

网络设备
14
DHCP服务器
16
自举服务器
18
协调器服务器
20
请求自举服务器的地址
404
提供自举服务器的列表
406
请求导引信息
408
提供导引信息
410
执行第一初始化
412
请求导引信息
414
提供导引信息
416
执行自举操作
418
建立安全管理连接
420
开始正常操作
422

图4