(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 102427484 A
(43)申请公布日 2012.04.25

(21)申请号 201110423043.7

(22)申请日 2011.12.16

(30)优先权数据
12/970371 2010.12.16 US

(71)申请人 微软公司
地址 美国华盛顿州

(72)发明人 R. 潘迪亚 A. 蒂瓦里
R. K. 阿马拉瓦迪

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 孙之刚 刘鹏

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

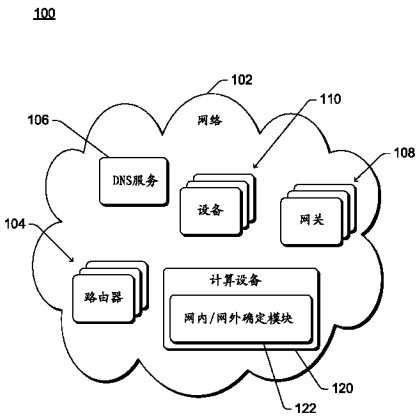
权利要求书 1 页 说明书 11 页 附图 5 页

(54)发明名称

基于 DNS 来确定设备是否处于网络内部

(57)摘要

在计算设备中产生和发送域名系统(DNS)查询,并且检查是否接收到经过核实的针对所述 DNS 查询的 DNS 响应。如果接收到经过核实的 DNS 响应,则确定计算设备处于特定网络内部,如果没有接收到经过核实的 DNS 响应,则确定计算设备处于该特定网络外部。如果 DNS 响应具有预期值并且所述 DNS 响应是经过可信机构数字签名的,则可以确定 DNS 响应是经过核实的,否则可以确定该 DNS 响应是没有经过核实的。



CN 102427484 A

1. 一种方法，包括：

产生（302）域名系统（DNS）查询；

促使（304）所述 DNS 查询被发送；

检查（312）是否接收到针对该 DNS 查询的经过核实的 DNS 响应；

如果接收到经过核实的 DNS 响应，则确定（316）计算设备处于特定网络内部；以及

如果没有接收到经过核实的 DNS 响应，则确定（318）计算设备处于特定网络外部。

2. 如权利要求 1 所述的方法，其中生成 DNS 查询包括产生包含特定名称的 DNS 查询，以及其中检查是否接收到经过核实的 DNS 响应包括检查 DNS 响应是否具有用于该特定名称的预期值。

3. 如权利要求 1 所述的方法，其中经过核实的 DNS 响应是从支持 DNS 安全扩展（DNSSEC）协议的 DNS 服务接收的。

4. 如权利要求 1 所述的方法，其中检查是否接收到经过核实的 DNS 响应包括检查接收到的 DNS 响应是否经过可信机构的数字签名。

5. 如权利要求 4 所述的方法，其中可信机构是特定网络的根证书机构。

6. 如权利要求 1 所述的方法，其中确定计算设备处于特定网络之外包括：如果在阈值数量的时间以内没有接收到针对 DNS 查询的 DNS 响应，则确定计算设备处于特定网络外部。

7. 如权利要求 1 所述的方法，还包括按照特定的间隔重复：促使 DNS 查询被发送，检查是否接收到经过核实的 DNS 响应，以及确定计算设备处于特定网络内部还是特定网络外部。

8. 一种计算设备，包括：

一个或多个处理器（502）；以及

一种或多种其上存储了多个指令的计算机可读媒体（504），其中所述指令在被所述一个或多个处理器执行时，促使一个或多个处理器：

接收（402）针对域名系统（DNS）查询的 DNS 响应；

检查（404）DNS 响应是否具有预期值；

检查（408）DNS 响应是否经过可信机构数字签名；以及

如果 DNS 响应具有预期值并且 DNS 响应是经过可信机构数字签名的，则确定（410）计算设备通过核实且处于特定网络内部；否则确定（406）计算设备未经核实并处于特定网络外部。

9. 如权利要求 8 所述的计算设备，其中预期值是基于 DNS 查询中的特定名称到计算设备已知的特定值的映射而被预期的值。

10. 如权利要求 8 所述的计算设备，其中特定网络包括公司网，并且其中可信机构是用于公司网的根证书机构。

基于 DNS 来确定设备是否处于网络内部

背景技术

[0001] 很多计算设备是能被很容易地运送到不同的位置的移动设备。这些移动设备有时可以根据其是否被认为处于特定网络内而以不同的方式工作。但是，在任何特定时间可靠确定移动设备何时处于特定网络内部是很困难的。

发明内容

[0002] 本发明内容是为了以简化形式引入精选概念而被提供的，并且在以下的具体实施方式部分中将会进一步描述这些概念。本发明内容的目的既不是识别所要求保护主题的关键特征或必要特征，也不是用来限制所要求保护的主题的范围。

[0003] 根据一个或多个方面，产生一个域名系统（DNS）查询并促使其被发送。执行关于是否接收到针对该 DNS 查询的经过核实的 DNS 响应的检查。如果接收到经过核实的 DNS 响应，则确定计算设备处于特定网络内部，如果没有接收到经过核实的 DNS 响应，则确定计算设备处于特定网络外部。

[0004] 根据一个或多个方面，对 DNS 查询的域名系统（DNS）响应将被接收。关于 DNS 响应是否具有预期值以及 DNS 响应是否由可信机构进行了数字签名的检查将被执行。如果 DNS 响应具有预期值并且 DNS 响应是经过可信机构数字签名的，则确定计算设备通过核实且处于特定网络内部，否则确定计算设备未经核实且处于特定网络外部。

附图说明

[0005] 在所有附图中，相同的数字被用于引用相同的特征。

[0006] 图 1 图示了根据一个或多个实施例来实现基于 DNS 确定设备是否处于网络内部的例示系统。

[0007] 图 2 图示了根据一个或多个实施例来实现基于 DNS 确定设备是否处于网络内部的另一个例示系统。

[0008] 图 3 是图示了根据一个或多个实施例用于计算设备基于 DNS 确定其是否处于特定网络内部的例示过程的流程图。

[0009] 图 4 是图示了根据一个或多个实施例用于计算设备核实 DNS 响应的例示过程的流程图。

[0010] 图 5 图示了可以被配置成根据一个或多个实施例来实现基于 DNS 确定设备是否处于网络内部的例示计算设备。

具体实施方式

[0011] 在这里讨论了基于 DNS 来确定设备是否处于网络内部。计算设备产生一个请求解析特定名称的域名系统（DNS）查询，并且将这个 DNS 查询发送到 DNS 服务。如果计算设备处于特定网络（例如公司网）内部，那么计算设备预期将接收到具有特定值的 DNS 响应，并且还会预期所述 DNS 响应是由可信机构进行了数字签名的。如果 DNS 响应具有预期的特定值，

并且是经过可信机构数字签名的，那么计算设备确定其处于特定网络内部。但是，如果 DNS 响应没有预期的特定值和 / 或未经过可信机构的数字签名，或者如果没有接收到 DNS 响应，那么计算设备确定其处于特定网络以外。

[0012] 在这里将会参考数字签名和数字证书。虽然数字签名和数字证书对于本领域技术人员来说是众所周知的，但是在这里包含了对它们的简要概述来为读者提供帮助。数字签名和数字证书通常是使用公钥密码术 (cryptography) 产生的。在公钥密码术中，实体 (例如用户、硬件或软件组件、设备、域等等) 具有与之关联的公钥 / 私钥对。公钥可以是可公开获得的，但是实体会将私钥保密。在没有私钥的情况下，使用公钥加密的数据在计算上是很难解密的。因此，数据可以由任一实体使用公钥来进行加密，并且只能由具有相应私钥的实体进行解密。此外，用于数据的数字签名可以使用数据和私钥来产生。在没有私钥的情况下，计算上很难创建可以使用公钥核实的签名。通过对公钥、签名以及带有签名的数据执行适当的数字签名核实算法，具有公钥的任何实体都可以使用公钥来核实数字签名。数字证书也是可以创建的，其中该数字证书包括实体的标识符和用于该实体的公钥，以及用实体私钥签名的数字证书，以便将实体的标识符绑定到该实体的公钥。

[0013] 可替换地，数字签名和数字证书可以使用对称密钥密码术来产生。在对称密钥密码术中，两个实体知道共享密钥 (也被称为对称密钥) 并将其保密。任何具有共享密钥的实体通常都能对使用共享密钥加密的数据进行解密。在没有共享密钥的情况下，计算上很难对使用共享密钥加密的数据进行解密。因此，如果两个实体全都知道共享密钥，那么每一个实体都可以加密数据，并且所述加密数据可以被另一个实体解密，但是如果其他实体不知道共享密钥，那么所述实体是不能解密该数据的。同样，具有共享密钥的实体可以对数据进行加密，并且该数据可以被该相同的实体解密，但是如果其他实体不知道共享密钥，那么所述其他实体是不能解密该数据的。此外，数字签名可以是基于对称密钥密码术产生的，例如使用带有密钥的散列 (keyed-hash) 消息验证 (authentication) 码机制。任何具有共享密钥的实体都可以产生和核实数字签名。例如，可信第三方可以基于特定实体的身份来产生对称密钥，然后可以为这个特定实体产生和核实数字签名 (例如通过使用对称密钥加密或解密数据)。数字证书可被创建，其中该数字证书包含了实体的标识符和用于该实体的公钥，以及经过数字签名的数字证书 (例如由可信第三方)，以便将实体的标识符绑定到该实体的公钥。

[0014] 图 1 图示了根据一个或多个实施例来实现基于 DNS 确定设备是否处于网络内部的例示系统 100。系统 100 包括网络 102，该网络是借助通信网络耦合在一起的一个或多个设备。通信网络可以包括有线和 / 或无线通信，并且允许网络 102 中的多种不同设备与网络 102 中的多种不同的其他设备进行通信。举例来说，通信网络可以是局域网 (LAN)、公共电话网、专用电话网、其他公共和 / 或专有网络、这些网络的组合等等。

[0015] 网络 102 包括多种不同的设备，这其中包括一个或多个路由器 104、一个或多个实现 DNS 服务 106 的设备、一个或多个网关 108 以及一个或多个其他设备 110。路由器 104 在网络 102 的多种不同设备之间路由数据分组或其他信息。如下文中更详细论述的那样，DNS 服务 106 将名称解析成网络地址。DNS 服务 106 通常是在一个或多个服务器上实现的，但是可替换地，DNS 服务 106 也可以在其他类型的设备上实现。网关 108 管理将网络 102 连接到其他网络 (例如因特网) 或网络 102 之外的其他设备。从网络 102 内部的设备到网络 102

外部的设备的通信以及从网络 102 外部的设备到网络 102 内部的设备的通信是由网关 108 管理的。

[0016] 设备 110 可以是多种不同类型的设备，这其中包括计算设备，例如台式计算机、服务器计算机、膝上或上网本计算机、平板或笔记本计算机、移动站、数据库或其他存储设备、娱乐电器、可通信地耦合到显示设备的机顶盒、电视或其他显示设备、蜂窝电话或其他无线电话、游戏控制台、汽车用计算机等等。设备 110 还可以是多种不同类型的输入设备，例如扫描仪、相机或其他图像捕获设备等等。设备 110 还可以是多种不同类型的输出设备，例如打印机、传真机、投影仪或其他显示设备等等。

[0017] 通常，网络 102 包括多个设备，这其中包括至少一个路由器 104、实现 DNS 服务 106 中的至少一部分的至少一个设备、至少一个网关 108 以及至少一个设备 110。然而应该指出的是，网络 102 可以包括任何数量的路由器 104、用于实现 DNS 服务 106 的至少一部分的任何数量的设备、任何数量的网关 108 以及任何数量的设备 110。此外还应该指出，并不是所有这些设备都必须包含在网络中(例如，在网络中可以不包含设备 110)。此外还应该指出，网络 102 的一个或多个这样的设备可以组合成单个设备。例如，路由器 104 和网关 108 的功能可以由单个设备提供。

[0018] 在例示系统 100 中，网络 102 还包括具有网内 / 网外确定模块 122 的计算设备 120。计算设备 120 也可以是设备 110 中的一个。该计算设备 120 可以是多种不同类型的计算设备，例如台式计算机、服务器计算机、膝上或上网本计算机、平板或笔记本计算机、移动站、数据库或其他存储设备、娱乐电器、可通信地耦合到显示设备的机顶盒、电视或其他显示设备、蜂窝电话或其他无线电话、游戏控制台、汽车用计算机等等。计算设备 120 通常是可以很容易移动到网络 102 内部的不同位置以及可以很容易在网络 102 内部的位置与网络 102 外部的位置之间移动的移动计算设备，例如蜂窝电话或其他无线电话、膝上或笔记本计算机等等。因此，网络 102 有时可以包括计算设备 120(当计算设备 120 处于网络 102 内部的时候)，而在其他时候则不包括计算设备 120 (当计算设备 120 处于网络 102 外部的时候)。虽然在系统 100 中示出的是单个计算设备 120，但是应该指出，在网络 102 中可以包括具有相同或不同设备类型的多个计算设备 120。

[0019] 网络 102 中包含的设备被配置成彼此经由通信网络来进行通信。这种设备配置可以在将设备添加到网络 102 中的时候执行，并且还可以在设备已被包含作为网络 102 的一部分之后的多种不同时间执行。网关 108 允许基于特定的策略和 / 或规则而在网络 102 包含的设备与网络 102 不包含的设备之间进行通信。网关 108 遵循的特定策略和 / 或规则可以基于网络 102 的所有者和 / 或设计人员、网络 102 的管理人员等等而改变。

[0020] 诸如计算设备 120 之类的计算设备通过连接到网络 102 来与网络 102 中的其他设备进行通信。连接到网络 102 指的是在计算设备与网络 102 之间建立通信链路。建立通信链路包括下列各项中的一项或多项：为计算设备获取网络地址(例如从网络 102 的动态主机配置协议(DHCP)服务器那里)，向网络 102 的域控制器验证计算设备或计算设备的用户(例如使用用户名和口令，使用数字证书等等)，与作为网络 102 的一部分包含的设备协商协议(例如与路由器 104 或网关 108)，与作为网络 102 的一部分包含的设备(例如网关 108)建立安全的(例如加密)通信信道等等。

[0021] 在计算设备与网络 102 之间建立通信链路可以由计算设备或别的设备(例如作为

网络 102 的一部分包含的设备)启动。一旦建立了通信链路,则计算设备可以与网络 102 中的其他设备进行通信(服从网络 02 中任何适当的访问控制策略)。

[0022] 诸如计算设备 120 之类的设备可被称为处于网络内部或网络外部。处于网络以内(也被称为处于网络内部)的设备是一个包含在网络中并且因此能在不必访问该网络以外的设备的情况下与该网络中包含的其他设备进行通信的设备。因此举例来说,路由器 104、网关 108、设备 112 以及在系统 100 中实现服务 106 的设备处于网络 102 内部,并且被配置成彼此之间经由网络 102 的通信网络来进行通信,而不必访问网络 102 以外的设备。处于网络 102 内部的设备可以经由网关 108 来与不在网络 102 内部的其他设备进行通信。此外还应该指出,虽然网络 102 内部的设备彼此之间可以经由通信网络进行通信,但是对于网络 102 内部的哪些设备可以访问网络 102 内部的其他哪些设备(或是访问方式)的多种不同访问控制限制也是可以实现的。

[0023] 处于网络以外(也被称为处于其外部)的设备是一个不在网络以内的设备。这种设备可以经由该网络的网关来与该网络内部的设备进行通信。因此举例来说,路由器 104、网关 108、设备 112 和实现服务 106 的设备可以经由网关 108 接收来自网络 102 外部的设备的通信(并且向其发送通信),以及服从网关 108 使用的策略和 / 或规则。

[0024] 哪些设备包括在网络 102 中可以采用不同的方式定义,并且可以至少部分基于实现网络 102 的实体和 / 或网络 102 的管理员的希望。在一个或多个实施例中,网络是由 DNS 服务 106 服务的设备定义的。网络 102 内部的设备向 DNS 服务 106 提交 DNS 查询,并且接收来自该服务的 DNS 响应。网络 102 外部的设备不能访问 DNS 服务 106(例如,网关 108 使用的策略和 / 或规则阻止该设备访问 DNS 服务 106)。

[0025] 在一个或多个其他实施例中,网络 102 是由能在不通过防火墙(例如由网关 108 或别的设备实现)进行通信或是没有访问因特网的情况下彼此访问的设备定义的。网络 102 内部的设备是那些能在没有通过防火墙通信或是接入因特网的情况下彼此访问的设备(服从网络 102 中任何适当的访问控制策略)。经由防火墙或因特网来与网络 102 内部的设备通信的设备则处于网络 102 的外部。

[0026] 此外,在一个或多个实施例中,网络 102 是一个由特定企业实体(例如特定公司,公司的特定部门或单位等等)管理或是为该特定企业实体管理的网络,因此被称为公司网。可替换地,网络 102 可以是其他类型的网络,例如家庭网络,教育网络,游戏网络等等。

[0027] 在系统 100 的示例中,计算设备 120 处于网络 102 之内。然而也有可能出现计算设备 120 变成处于网络外部的情形。例如,计算设备 120 可以移动到不同的位置,并且计算设备 120 在该位置不能以使得计算设备 120 处于网络 102 内部的方式来与网络 102 建立通信链路。应该指出的是,在使用计算设备 120 的所有地方,计算设备 120 可以多次在网络 102 的内部与网络 102 的外部之间移动。

[0028] 图 2 图示了根据一个或多个实施例实现基于 DNS 确定设备是否处于网络内部的另一个例示系统 200。系统 200 与图 1 的系统 100 相似,其包括网络 102、一个或多个路由器 104、DNS 服务 106、一个或多个网关 108 以及一个或多个其他设备 110。系统 200 还包括计算设备 120。虽然在系统 200 中示出了单个计算设备 120,但是应该指出,在系统 200 中可以包括具有相同或不同设备类型的多个计算设备 120。

[0029] 图 2 的计算设备 120 是图 1 的计算设备 120。在图 1 中,计算设备 120 包含在网

络 102 内部。然而在图 2 中，计算设备 120 处于网络 102 外部，并且经由网关 108 来与网络 102 建立通信链路。在计算设备 120 与网关 108 之间可以经由多种其他设备或通信网络来建立通信链路，例如经由因特网、经由蜂窝网络或其他公共网络等等。

[0030] 计算设备 120 可以基于所述计算设备 120 确定其处于网络 102 的内部还是网络 102 的外部而以不同的方式工作。例如，计算设备 120 可以基于该计算设备 120 是否处于网络 102 的内部来决定是否使用加密通信，计算设备 120 可以基于该计算设备 120 是否处于网络 102 的内部来允许或禁用某个功能，计算设备 120 可以基于该计算设备 120 是否处于网络 102 的内部来允许或拒绝访问存储在计算设备 120 上的文件等等。基于计算设备 120 是否处于网络 102 的内部，例如基于计算设备 120 和 / 或运行在计算设备 120 上的软件或固件的设计，计算设备 120 可以可选地做出多种不同的其他决定或是执行多种不同的其他操作或功能。

[0031] 计算设备 120 包括用于在任何特定时间确定计算设备 120 处于网络 102 的内部还是网络 102 的外部的网内 / 网外确定模块 122。为了执行这种判定，网内 / 网外确定模块 122 利用 (leverage)DNS 系统和 DNS 服务 106。DNS 系统允许使用域名(例如包含在统一资源定位符(URL)中)来识别设备或服务，其中与网络地址(例图网际协议(IP)v4 或 v6 地址)相比，域名通常更易于用户使用和引用。一个或多个 DNS 服务 106 通过操作来将诸如域名之类的特定名称映射到可被计算设备 120 用以访问特定设备或服务的对应的网络地址。这种名称到对应网络地址的映射也被称为 DNS 解析。

[0032] 在一个或多个实施例中，这里论述的 DNS 系统指的是符合众所周知的 DNS 协议(例如在网络工作组请求注释 1034(1987 年 11 月)以及网络工作组请求注释 1035(1987 年 11 月)中论述的协议)的系统。然而应该指出的是，这里论述的基于 DNS 来确定设备是否处于网络内部的技术可以与执行类似功能的其他系统或协议结合使用。

[0033] DNS 服务 106 还支持多种不同安全功能，因此保护 DNS 服务 106 能够提供的多种不同信息或数据的安全。这种功能包括支持用于 DNS 响应的数字签名，其中该响应是 DNS 服务响应于 DNS 查询返回的。用于 DNS 响应的数字签名可以由 DNS 服务 106 本身产生(例如使用 DNS 服务的私钥)，或者可替换地可以由另一个设备或组件产生(例如使用 DNS 服务 106 信任的另一个实体的私钥)。

[0034] 在一个或多个实施例中，DNS 服务 106 支持众所周知的 DNS 安全扩展(DNSSEC)协议。关于 DNSSEC 协议的附加信息可以在网络工作组请求注释 4033(2005 年 3 月)、网络工作组请求注释 4034(2005 年 3 月)以及网络工作组请求注释 4035(2005 年 3 月)中找到。

[0035] 通常，网内 / 网外确定模块 12 通过向 DNS 服务发送 DNS 查询来确定计算设备 120 处于网络 102 的内部还是网络 102 的外部。这个 DNS 查询是一个请求解析特定名称(例如域名或其他名称)的请求。如果计算设备 120 处于网络 102 内部，那么 DNS 查询将被路由至 DNS 服务 106。然而，如果计算设备 120 处于网络 102 的外部，那么 DNS 查询将被路由至另一个 DNS 服务(未显示)，例如因特网上可以公开获得的 DNS 服务。网内 / 网外确定模块 122 可以被配置成具有 DNS 查询将被送抵的 DNS 服务的网络地址，或者可以采用别的方式来获取 DNS 服务的网络地址(例如从网关 108)。可替换地，模块 122 可以将 DNS 查询转发到另一个模块或服务，例如本地 DNS 解析器，其中所述模块或服务知道(或获取)DNS 服务的网络地址，并且代表模块 122 来将 DNS 查询转发到 DNS 服务。

[0036] DNS服务106维护关于DNS查询中的特定名称所映射到的特定值的记录，或者可以采用其他方式来访问该记录。该特定名称通常被映射到一个特定的值，但是作为替换，它也可以被映射到多个不同的特定值。用于该特定名称的映射通常是由DNS服务106秘密地或者私下里维护，并且该映射不会被暴露给网络102外部的DNS服务。例如，用于这个特定名称的映射并未在因特网上或者向网络102外部的其他DNS服务注册。但是，网内/网外确定模块122还知道用于该特定名称的映射。所述网内/网外确定模块122可以被配置成具有或以其他方式获取用于该特定名称的映射。

[0037] DNS服务向网内/网外确定模块122返回DNS响应。如果DNS响应是由DNS服务106生成或返回的，那么DNS响应包括DNS查询中的特定名称所映射到的特定值。然而，如果DNS响应是由网络102外部的DNS服务生成或返回的，那么DNS响应将会包括一个表明不能映射DNS查询中的特定名称的指示(或者包括不正确的映射)，例如包括一个“DNS名称不存在”错误的指示。可替换地，如果计算设备120处于网络102的外部，那么网络102外部的DNS服务都不能返回响应，因此网内/网外确定模块122不会接收到DNS响应。

[0038] 此外，DNS服务106返回的DNS响应是由可信机构数字签名的。由可信机构数字签名的DNS响应可以指被可信机构数字签名的整个DNS响应，或者可替换地是由可信机构数字签名的DNS响应的一部分(例如DNS查询中的特定名称被映射到的特定值)。网内/网外确定模块122可以采用多种不同的方式验证或已经验证了数字签名(例如通过使用可信机构的公钥)。该可信机构是计算设备120和/或网内/网外确定模块122信任的实体。所述可信机构可被包含作为网络102的一部分，或者可替换地可以处于网络102的外部。该可信机构可以是产生或返回DNS响应的DNS服务106。可替换地，该可信机构可以是另一个实体，例如用于网络102的根证书机构。如果DNS响应是由DNS服务106产生或返回的，那么DNS响应将会由可信机构数字签名。但是，如果DNS响应是由网络102外部的DNS服务产生或返回的，那么DNS响应不会被可信机构数字签名。

[0039] 网内/网外确定模块122使用DNS响应(或该响应的缺失)来确定计算设备120是否处于网络102内部。如果计算设备120处于网络102内部，那么DNS响应将会包括DNS查询中的特定名称被映射到的特定的值，并且DNS响应也会由可信机构数字签名。模块122知道DNS查询中的特定名称应该映射到的特定值，并且这个值也被称为预期值(模块122预期包含在DNS响应中的值)。

[0040] 因此，如果DNS响应同时包括预期值并由可信机构数字签名，那么网内/网外确定模块122确定计算设备120处于网络102的内部。但是，如果DNS响应不包括预期值和/或未经过可信机构数字签名，或者如果没有接收到DNS响应，那么网内/网外确定模块122确定计算设备120处于网络102的外部。

[0041] 在替换实施例中，如果DNS响应包括预期值，那么无论DNS响应是否经过可信机构数字签名，网内/网外确定模块122都会确定计算设备120处于网络102内部。在其他替换实施例中，如果DNS响应是经过可信机构数字签名的，那么无论DNS响应是否包括预期值，网内/网外确定模块122都会确定计算设备120处于网络102内部。

[0042] 图3是图示根据一个或多个实施例的可供计算设备用来基于DNS来确定其是否处于特定网络内部的例示过程300的流程图。过程300可以在软件、固件、硬件或是其组合中实现。图3的左侧示出的过程300的动作是由计算设备执行的，例如图1和2的计算设备

120，并且通常由该计算设备上的网内 / 网外确定模块(例如图 1 的模块 122)执行的。在图 3 的右侧示出的过程 300 的动作是由 DNS 服务执行的，例如图 1 和 2 的 DNS 服务 106。过程 300 被显示成是一组动作，并且不局限于所显示的用于执行多种不同动作的操作的顺序。过程 300 是一个供计算设备用来确定其是否处于特定网络内部的例示过程；在这里通过参考不同的附图包含了关于计算设备确定其是否处于特定网络内部的附加论述。

[0043] 在过程 300 中，计算设备产生 DNS 查询(动作 302)。该 DNS 查询是一个要求解析特定名称的查询，并且如果计算设备处于特定网络内部，那么该计算设备预计一个特定值会返回。这个特定名称可以是 URL 或可替换地是别的名称。例如，这个特定名称可以采用“insideoutside.<domain-name>”的形式，其中“insideoutside”将 DNS 查询标识成是用以确定计算设备是否处于特定网络内部的查询，并且“<domain-name>”标识该特定的网络。

[0044] 网内 / 网外确定模块促使 DNS 查询被发送到 DNS 服务(动作 304)。该网内 / 网外确定模块可以通过发送 DNS 查询或可替换地促使别的模块或组件发送 DNS 查询来促使所述 DNS 查询被发送。

[0045] 所述 DNS 查询由 DNS 服务接收(动作 306)。接收这个 DNS 查询的 DNS 服务可以基于计算设备的位置而改变，例如基于计算设备是否处于特定网络内部。

[0046] DNS 服务产生对接收到的 DNS 查询的 DNS 响应(动作 308)。在一个或多个实施例中，如果 DNS 服务处于特定网络内部，那么 DNS 响应包括计算设备预期的并由可信机构数字签名的特定值。但是，如果 DNS 服务处于特定网络外部，那么 DNS 响应不会包括特定值和 / 或不会经过可信机构数字签名。

[0047] DNS 服务向计算设备发送 DNS 响应(动作 310)。该 DNS 服务可以发送 DNS 响应或者可替换地促使别的设备或组件发送 DNS 响应。可替换地，如果 DNS 服务处于网络外部，那么 DNS 服务可以不在动作 308 和 310 产生和返回 DNS 响应。

[0048] 网内 / 网外确定模块检查是否接收到经过核实的 DNS 响应(动作 312)。有可能发生这样的情形，其中包含网内 / 网外确定模块的计算设备处于网络的外部，并且因此不会接收到 DNS 响应或者接收到未通过核实的 DNS 响应。如果接收到 DNS 响应，那么网内 / 网外确定模块可以通过自己接收 DNS 响应，或者可替换地通过调用或者促使别的模块或组件接收 DNS 响应来促使 DNS 响应被接收。此外，如果接收到 DNS 响应，那么会在动作 312 核实 DNS 响应。DNS 响应可以用不同的方式核实，例如通过检查 DNS 响应是否包含用于包含在 DNS 查询中的特定名称的预期值，和 / 或 DNS 响应是否经过可信机构数字签名。

[0049] 过程 300 基于是否接收到经过核实的 DNS 响应的检查来进行(动作 314)。如果接收到经过核实的 DNS 响应，则确定计算设备处于特定网络内部(动作 316)。

[0050] 然而，如果没有在阈值时间量以内接收到 DNS 查询，那么网内 / 网外确定模块超时，并且计算设备被确定为处于特定网络外部(动作 318)。这个阈值时间量是可以改变的(例如 1 秒、5 秒等等)。此外，如果接收到 DNS 响应但是该 DNS 响应没有通过核实，则确定该计算设备处于特定网络以外(动作 318)。

[0051] 然后，计算设备处于特定网络内部还是特定网络外部的判定可被转发或以其他方式使得对于计算设备的其它多种不同的组件或模块是可得到的。之后，这些其他组件或模块可以基于计算设备处于特定网络内部还是特定网络外部来以多种不同的方式进行操作。

[0052] 该过程 300 可以在特定的间隔重复进行，包括规则或不规则的间隔。例如，过程

300 可以大约每五分钟、大约每小时等等执行一次。另举一例，过程 300 可以响应于特定事件而执行，例如响应于计算设备从节能模式（例如从休眠或冬眠模式中）中恢复操作，响应于检测（例如通过计算设备的全球定位系统（GPS））到计算设备的移动超出阈值数量（例如 100 码、1 英里等等），响应于计算设备的网络接口的建立或移除（例如计算设备的网络接口被使能），响应于计算设备确定该计算设备处于新的无线网络范围以内或者不再处于其先前所处的无线网络的范围以内等等。

[0053] 图 4 是示出了根据一个或多个实施例来供计算设备用来核实 DNS 响应的例示过程 300 的流程图。过程 400 可以在软件、固件、硬件或是其组合中实现。过程 400 是由计算设备 100 执行的，例如图 1 和 2 中的计算设备 120，并且通常是由该计算设备上的网内 / 网外确定模块（例如图 1 和 2 的模块 122）执行的。举例来说，过程 400 可以是图 3 的动作 312 和 314。过程 400 被显示成是一组动作，并且其不受所显示的用于执行多种不同动作的操作的顺序的限制。过程 400 是一个供计算设备用来核实 DNS 响应的例示过程；在这里通过参考不同的附图包含了关于计算设备核实 DNS 响应的附加论述。

[0054] 在过程 400 中，DNS 响应将被接收（动作 402）。该 DNS 响应是从 DNS 服务（或可替换地是下文中更详细论述的 DNS 缓存）或是从实现过程 400 的设备的其他模块或组件（例如由网内 / 网外确定模块调用或是促使接收 DNS 响应的别的模块或组件）那里接收的。

[0055] 检查 DNS 响应是否包括一个作为预期值的值（动作 404）。如上所述，如果计算设备是特定网络的一部分，那么 DNS 响应将会包括用于 DNS 查询中的特定名称的预期值，其中所述 DNS 响应是针对所述 DNS 查询的响应。此外，在动作 404 中可以使用多个不用的预期值，并且在这里将会检查 DNS 响应是否包括所述多个不同的预期值中的一个或多个预期值。

[0056] 如果 DNS 响应不包括预期值，那么 DNS 响应未经核实的或是没有通过核实（动作 406）。

[0057] 然而，如果 DNS 响应包括预期值，则检查 DNS 响应是否经可信机构数字签名（动作 408）。这个可信机构可以是 DNS 服务或是如上所述的其他可信实体。

[0058] 如果 DNS 响应没有经过可信机构的数字签名，那么 DNS 响应是未经核实或是没有通过核实（动作 406）。但是，如果 DNS 响应是经过可信机构数字签名的，那么 DNS 响应是经过核实的（动作 410）。

[0059] 回到图 1 和 2，在一个或多个实施例中，计算设备 120 维护 DNS 缓存。这个 DNS 缓存是特定名称到已经被 DNS 服务解析并返回给计算设备 120 的特定值的映射的本地拷贝。因此可能出现这样的情形，其中网内 / 网外确定模块 122 发送 DNS 查询来解析特定名称，并且用于所述特定名称的映射被包含在 DNS 缓存内。在这种情形下，网内 / 网外确定模块 122 是基于 DNS 缓存中的映射而不是来自 DNS 服务的映射来接收 DNS 响应。举个例子，参考图 3，动作 304 中的 DNS 查询将被发送到 DNS 缓存，并且动作 312 中的 DNS 响应是从 DNS 缓存接收的。

[0060] 在一个或多个实施例中，计算设备 120 被配置成避免出现网内 / 网外确定模块 122 由于以 DNS 缓存中的映射为基础的 DNS 响应而不正确地确定计算设备 120 是否处于特定网络内部这样的情形。这种情形可以采用不同的方式来避免。

[0061] 在一个或多个实施例中，DNS 缓存中的每一个映射都具有相关联的生存时间（TTL），对于 DNS 缓存中的不同映射来说，该生存时间既可以是相同的，也可以是不同的。在

用于 DNS 缓存中的映射的生存时间期满之后，用于解析包含在过期映射中的特定名称的 DNS 查询将被转发到 DNS 服务，以便解析而不是仅仅基于 DNS 缓存中的映射来返回 DNS 响应。对用于确定计算设备 120 是否包含在特定网络中的特定名称的映射来说，其生存时间被设置成了一个很小的值(例如零值，小于 5 分钟的值等等)。因此，通过对于 DNS 缓存中的这种映射具有很短的生存时间，网内 / 网外确定模块 122 不会在过长的时段中依赖于 DNS 缓存中的不正确的过期数据。

[0062] 可替换地，DNS 缓存可以不维护用于确定计算设备 120 是否处于特定网络内部的特定名称的映射，并且在 DNS 缓存中不维护包含了这种映射的针对 DNS 查询的 DNS 响应。这也可以被视为是用于确定计算设备是否处于特定网络内部的特定名称的映射具有大小为零的生存时间。例如，DNS 缓存可以不维护格式为“insideoutside.<domain-name>”的映射。因此，通过在 DNS 缓存中不具有这种映射，网内 / 网外确定模块 122 不会依靠 DNS 缓存中的不正确数据。

[0063] 应该指出的是，虽然所示出的是单个网络 102，但是这里论述的确定设备是否处于网络内部的技术可以与多个不同的网络一起使用。计算设备 120 可以被配置成具有或以其他方式获取用于多种不同网络中的每一个网络的可信机构的指示(并且可选地获取 DNS 服务的网络地址)。网内 / 网外确定模块 122 因此能够很容易在任何特定时间确定计算设备 120 处于那些不同网络中的任一网络的内部还是外部。

[0064] 此外，应该指出的是，虽然网内 / 网外确定模块 122 被显示成是计算设备 120 的一部分，但是可替换地，网内 / 网外确定模块 122 的多种不同功能可以实现在其他设备上。例如，计算设备 120 可以与可以是网络 120 或别的网络的一部分的一个或多个其他设备或服务进行通信，其中这些设备或服务可以执行这里论述的用于确定设备是否处于网络内部的技术的多种不同方面。

[0065] 因此，这里论述的基于 DNS 来确定设备是否处于网络内部的技术允许计算设备在任何特定时间精确和可靠地确定计算设备是否处于特定网络内部。通过使用 DNS 系统，这里论述的基于 DNS 来确定设备是否处于网络内部的技术使用了已有的可靠系统来做出判定。DNS 系统用已经作为一个可靠的系统工作，其通过酌情提供复制、备份等来保持 DNS 功能的高可用性。因此，不需要构造和保持可用性很高的附加可靠系统来实现这里论述的基于 DNS 确定设备是否处于网络内部的技术。

[0066] 更进一步，这里论述的基于 DNS 确定设备是否处于特定网络内部的技术是在不同类型的网络部署中工作的。例如，这里论述的基于 DNS 确定设备是否处于特定网络内部的技术可以与网际协议(IP)版本 4 (IPv4)网络地址、IP 版本 6 (IPv6)网络地址、站内自动隧道寻址协议(ISATAP)地址和机制、其他协议和 / 或机制、上述各项的组合等等一起使用。

[0067] 这里论述的基于 DNS 确定设备是否处于特定网络内部的技术支持多种不同的使用场景。例如，计算设备可以在“始终启动”访问模式中工作，在该模式中，无论是否移动到在特定网络内部和特定网络外部之间变化的不同位置，计算设备都保持与特定网络(例如企业网)的连接。计算设备可以继续工作，因此在任何时间确定该计算设备处于网络内部还是外部，并且基于该判定来酌情采用不同的方式工作。

[0068] 图 5 图示了可以根据一个或多个实施例被配置成实现基于 DNS 确定设备是否处于网络内部的例示计算设备 500。举例来说，计算设备 500 可以是图 1 和 2 的计算设备 120，

或是图 1 和 2 的一个或多个路由器 104、DNS 服务 106、网关 108 和 / 或设备 110。

[0069] 计算设备 500 包括一个或多个处理器或处理单元 502，可以包括一个或多个存储器和 / 或存储组件 506 的一个或多个计算机可读媒体 504，一个或多个输入 / 输出（I/O）设备 508，以及允许多种不同的组件和设备彼此通信的总线 510。计算机可读媒体 504 和 / 或一个或多个 I/O 设备 508 可被包含作为计算设备 500 的一部分，或者可替换地它也可以耦合到计算设备 500。总线 510 代表了若干种类型的总线结构中的一种或多种，包括使用了多种不同总线架构的存储器总线或存储器控制器，外设总线，图形加速端口，处理器或本地总线等等。总线 510 可以包括有线和 / 或无线总线。

[0070] 存储器 / 存储组件 506 代表一个或多个计算机存储媒体。组件 506 可以包括易失媒体（例如随机存取存储器（RAM））和 / 或非易失媒体（例如只读存储器（ROM）、闪存、光盘、磁盘等等）。组件 506 可以包括固定媒体（例如 RAM、ROM、固定硬盘驱动器等等）以及可移除媒体（例如闪存驱动器、可移除硬盘驱动器、光盘等等）。

[0071] 这里论述的技术可以在软件中利用由一个或多个处理单元 502 运行的指令实现。应该了解的是，不同的指令可以存储在计算设备 500 的不同组件中，例如存储在处理单元 502，处理单元 502 的多种不同缓存存储器，设备 500 的其他缓存存储器（未显示）或是其他计算机可读媒体等等中。此外，应该了解的是，在计算设备 500 中存储指令的位置是可以随时间改变的。

[0072] 一个或多个输入 / 输出设备 508 允许用户在计算设备 500 中输入命令和信息，并且还允许将信息呈现给用户和 / 或其他组件或设备。输入设备的示例包括键盘、光标控制设备（例如鼠标）、麦克风、扫描仪等等。输出设备的示例包括显示设备（例如监视器或投影仪）、扬声器、打印机、网卡等等。

[0073] 在这里，多种不同的技术可以是在软件或程序模块的上下文中描述的。通常，软件包括执行特定任务或实现特定抽象数据类型的例程、应用、程序、对象、组件、数据结构等等。这些模块和技术的实现方式可以存储在某种类型的计算机可读媒体上，或是经过此类媒体来传送。计算机可读媒体可以是能被计算设备访问的任何可用介质或媒体。作为示例而不是限制，计算机可读媒体可以包括“计算机存储媒体”和“通信媒体”。

[0074] “计算机存储媒体”包括通过任何用于存储信息的方法或技术实现的易失和非易失、可移除和不可移除媒体，所述信息例如是计算机可读指令、数据结构、程序模块或其他数据。计算机存储媒体包括但不局限于 RAM，ROM，EEPROM，闪存或其他存储器技术，CD-ROM，数字多用途盘（DVD）或其他光学存储器，磁带盒，磁带，磁盘存储器或其他磁存储设备，或是其他任何可以用于存储期望信息并能被计算机访问的介质。

[0075] “通信媒体”通常会将计算机可读指令、数据结构、程序模块或其他数据包含在诸如载波或其他传输机制之类的调制数据信号中。通信媒体还包括任何信息递送媒体。术语“调制数据信号”指的是这样的信号，其一个或多个特性以在该信号中编码信息的方式而被设置或改变。作为示例而不是限制，通信媒体包括诸如有线网络或直接线路连接之类的有线媒体以及诸如声学、RF、红外以及其他无线媒体之类的无线媒体。上述各项的任何组合都包含在计算机可读媒体的范围以内。

[0076] 一般来说，这里描述的任何功能或技术都可以使用软件、固件、硬件（例如固定逻辑电路）、手动处理或是这些实现方式的组合来实现。这里使用的术语“模块”和“组件”通

常代表的是软件、固件、硬件或是其组合。在软件实施方式的情况下，模块或组件代表当在处理器(例如一个或多个 CPU)上运行时执行指定任务的程序代码。程序代码可以存储在一个或多个计算机可读存储设备中，对它更进一步的描述可以参考图 5 找到。这里论述的基于 DNS 确定设备是否处于网络内部的技术的特征是不依赖于平台的，这意味着这些技术可以在具有多种处理器的多种商业计算平台上实现。

[0077] 虽然通过特定于结构特征和 / 或方法动作的语言描述了本主题，但是应该理解，附加权利要求中的主题未必局限于上述具体特征或动作。相反，以上描述的具体特征和动作是作为用于实现权利要求的例示形式公开的。

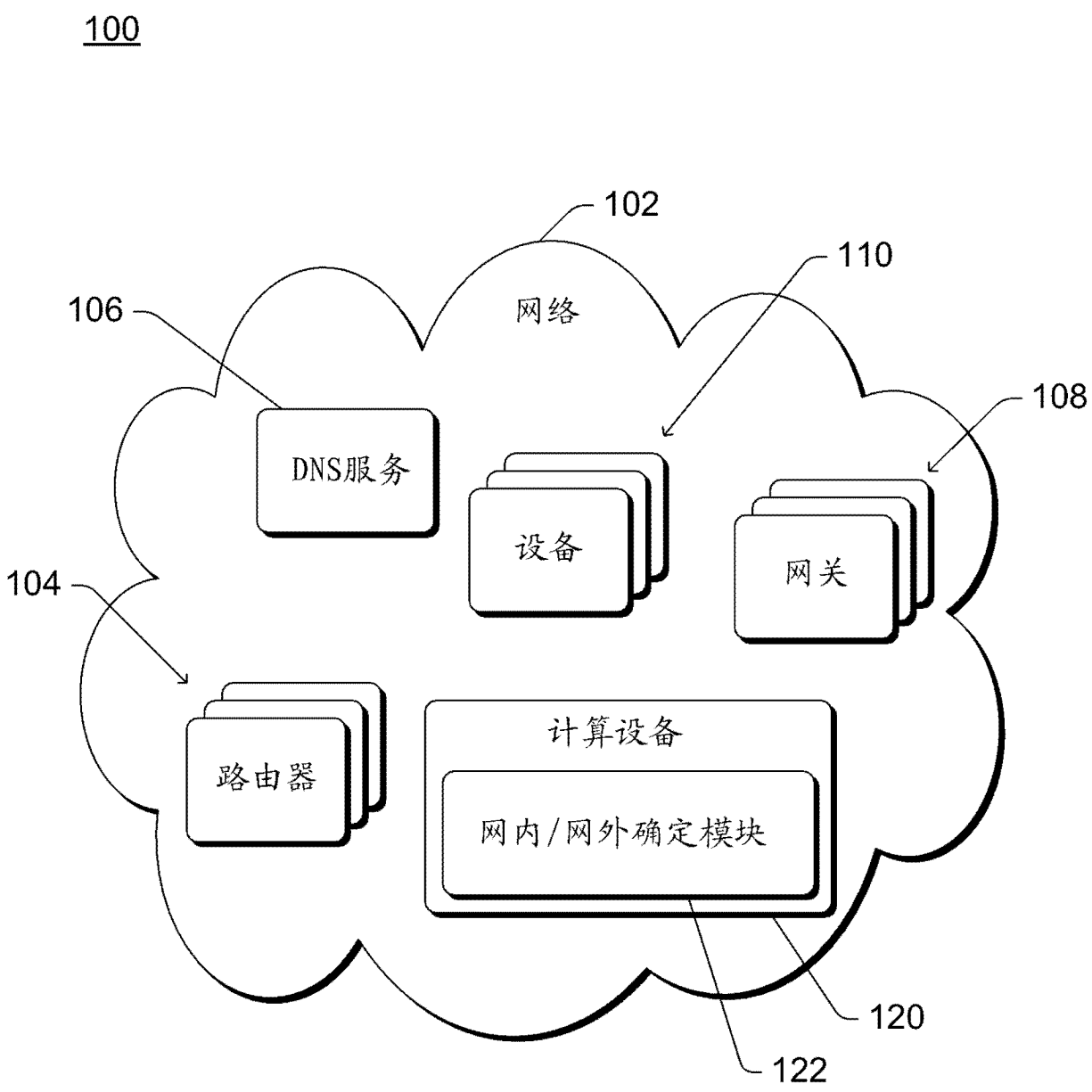

100
102
网络
110
106
108
DNS服务
设备
网关
104
路由器
计算设备
网内/网外确定模块
120
122

图 1

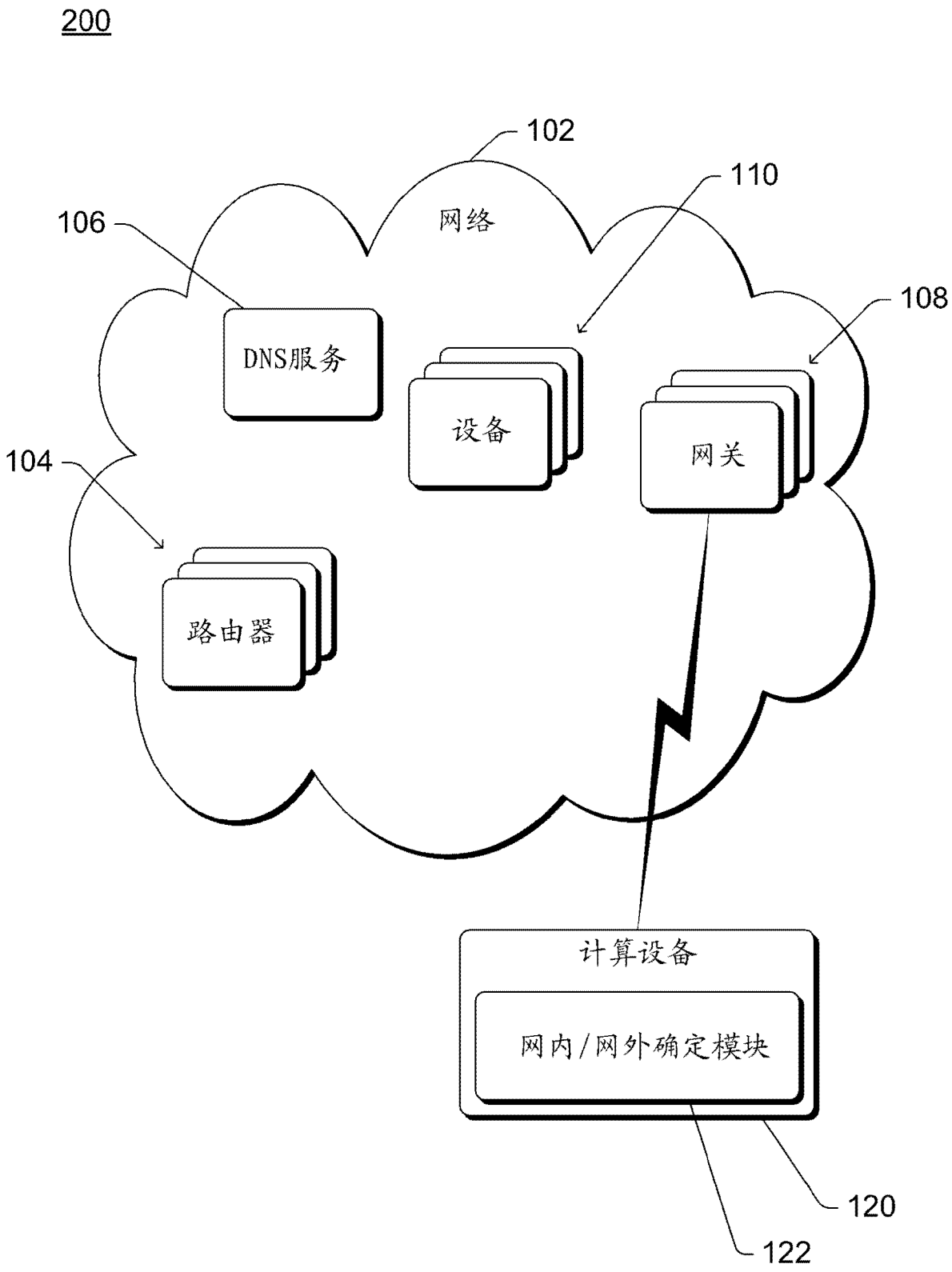

200
102
网络
110
106
108
DNS服务
设备
网关
104
路由器
计算设备
网内/网外确定模块
120
122

图 2

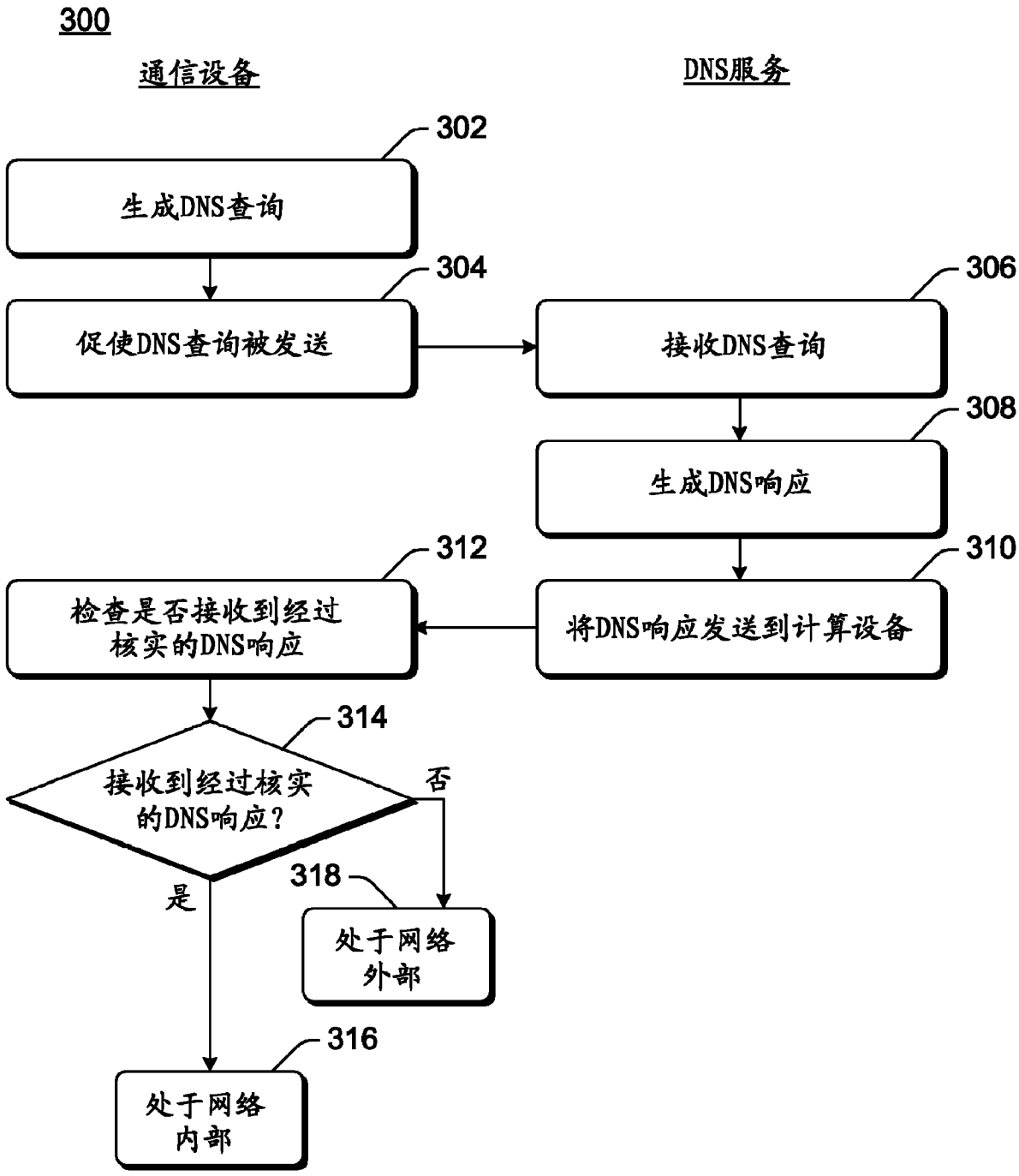

300
通信设备
DNS服务
302
生成DNS查询
304
促使DNS查询被发送
306
接收DNS查询
308
生成DNS响应
310
将DNS响应发送到计算设备
312
检查是否接收到经过核实的DNS响应
314
接收到经过核实的DNS响应？
否
是
318
处于网络外部
316
处于网络内部

图 3

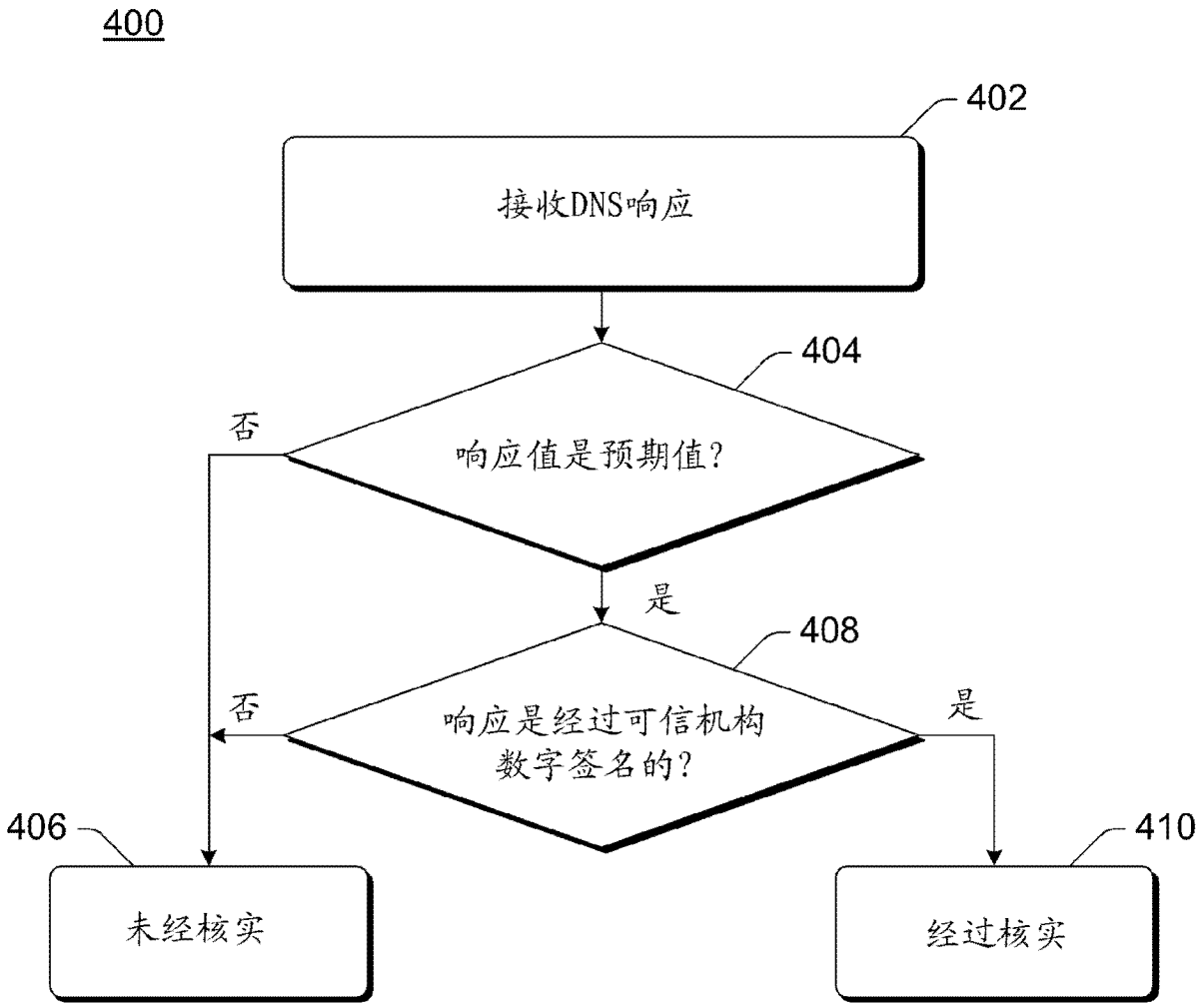

400
402
接收DNS响应
404
响应值是预期值?
否
是
408
响应是经过可信机构数字签名的?
否
是
406
未经核实
410
经过核实

图 4

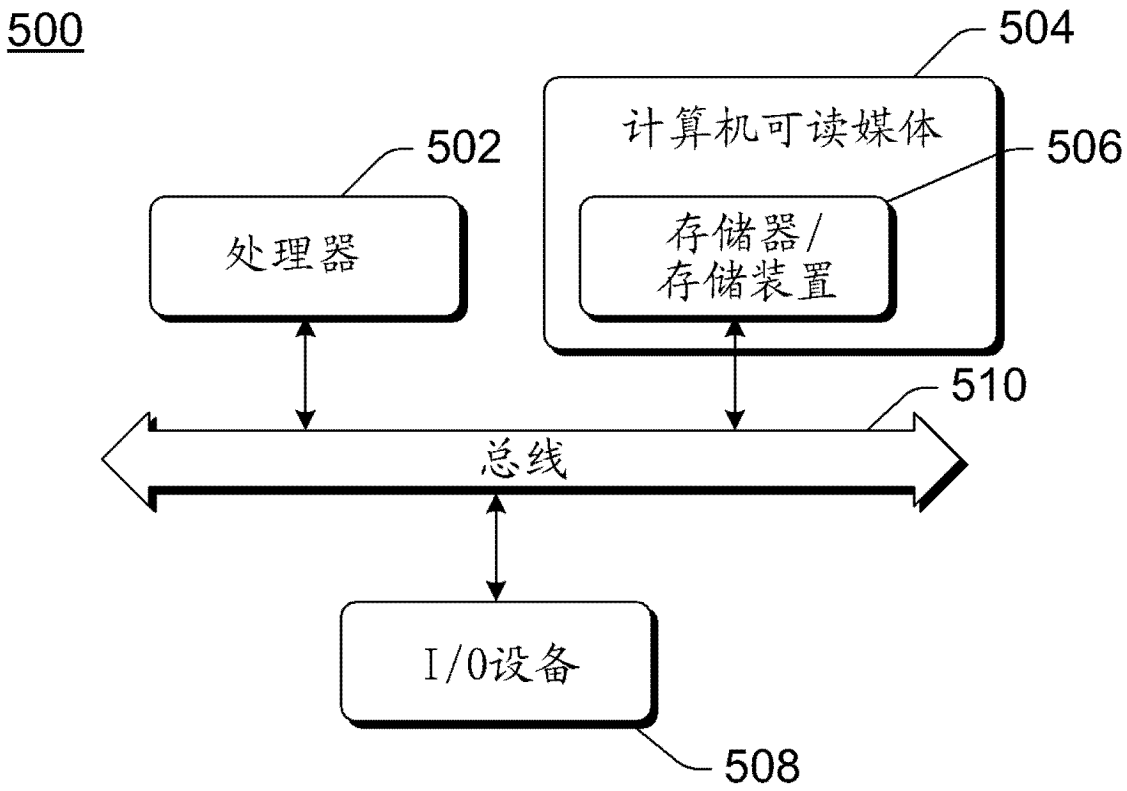


图 5