(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102112979 B
(45)授权公告日 2015.05.27

(21)申请号 200980130777.7
(22)申请日 2009.07.20
(30)优先权数据
12/189,034 2008.08.08 US
(85)PCT国际申请进入国家阶段日
2011.01.28
(86)PCT国际申请的申请数据
PCT/US2009/051143 2009.07.20
(87)PCT国际申请的公布数据
WO2010/017025 EN 2010.02.11
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 R·M·特蕾西 L·梅伦
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 黄嵩泉 钱静芳
(51)Int.Cl.
*H04L 29/12*(2006.01)
(56)对比文件
US 2006/0129665 A1,2006.06.15, 摘要、权利要求1-11、说明书第16-57段、附图1-4.
US 6560634 B1,2003.05.06, 全文.
CN 101087253 A,2007.12.12, 全文.
审查员 王晓燕

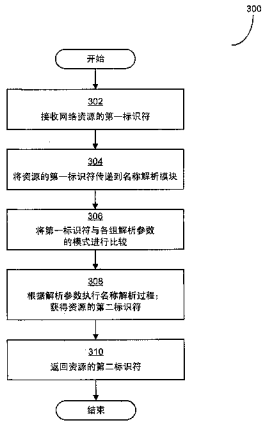
权利要求书2页 说明书17页 附图11页

(54)发明名称

安全资源名称解析

(57)摘要

用于保证名称解析技术的安全且用于确保名称解析技术能在具有可经由单个网络接口访问的多个覆盖网络的现代网络中运作的技术。根据此处所描述的原理中的某一些,可由诸如最终用户或管理员等用户实现一组解析参数,该组解析参数在名称解析过程中使用来保护该过程的安全和/或在覆盖网络中进行该过程。在某些实现中,该组解析参数可作为规则表来维护,并用于支配名称解析过程。例如,可创建解析参数来支配DNSSEC会话,或支配如何与用微软的直接访问覆盖技术实现的网络进行通信,或支配使用任何其他联网技术的通信。




CN 102112979 B

1. 一种名称解析方法，包括：

(A) 接受网络资源的第一标识符作为输入；

(B) 咨询各组解析参数的集合来确定适用于所述第一标识符的一组适用的解析参数，所述一组适用的解析参数支配主机计算设备与所述主机计算设备向其发出名称解析请求的远程计算设备之间的通信，其中咨询所述各组解析参数的集合包括：

(B1) 将所述网络资源的第一标识符与和所述各组解析参数的每一组相关联的模式进行比较以确定每一组解析参数是否适用于所述第一标识符；以及

(C) 从所述远程计算设备获得所述网络资源的第二标识符，所述获得包括进行名称解析过程来基于所述第一标识符确定所述网络资源的第二标识符，其中所述名称解析过程由所述一组适用的解析参数来支配。

2. 如权利要求 1 所述的方法，其特征在于，所述获得还包括：

(C1) 根据所述一组适用的解析参数向所述远程计算设备发送一名称解析请求。

3. 如权利要求 1 所述的方法，其特征在于，所述第一标识符是所述网络资源的文本标识符，所述第二标识符是所述网络资源的数字标识符。

4. 如权利要求 1 所述的方法，其特征在于，所述解析参数包括关于要使用的一种或多种类型的加密的信息。

5. 如权利要求 1 所述的方法，其特征在于，所述解析参数包括在所述名称解析过程期间要与其交换信息的一个或多个网络资源的标识符。

6. 如权利要求 1 所述的方法，其特征在于，所述名称解析过程是根据域名系统 DNS 协议的过程。

7. 如权利要求 6 所述的方法，其特征在于，所述名称解析过程是根据 DNS 安全扩展 DNSSEC 协议的过程。

8. 如权利要求 6 所述的方法，其特征在于，所述名称解析过程适用于与使用直接访问实现的覆盖网络一起运作。

9. 一种名称解析方法，所述方法包括：

(A) 从应用程序接受能经由网络访问的网络资源的域名作为输入；

(B) 从各组解析参数的集合中确定一组适用的解析参数，其中从所述各组解析参数的集合中确定所述一组适用的解析参数包括将所述网络资源的域名与和所述各组解析参数中的每一组相关联的模式进行比较来确定所述一组解析参数是否适用于所述域名；

(C) 根据所述一组适用的解析参数建立到网络上的域名服务 DNS 服务器的连接；

(D) 根据所述一组适用的解析参数将 DNS 查询传递到所述 DNS 服务器；

(E) 从所述 DNS 服务器接收包括所述网络资源的数字标识符的响应；以及

(F) 将所述数字标识符提供给所述应用程序。

10. 如权利要求 9 所述的方法，其特征在于，建立到 DNS 服务器的连接的动作包括：建立到由所述一组适用的解析参数所标识的 DNS 服务器的连接。

11. 如权利要求 9 所述的方法，其特征在于，所述方法还包括：

确认所述响应是根据所述解析参数生成的；以及

如果所述响应不是根据所述解析参数生成的，则不将所述数字标识符提供给所述应用程序。

12. 如权利要求 9 所述的方法，其特征在于，确认所述响应是根据所述解析参数生成的包括确定所述响应是否根据 DNS 安全扩展 DNSSEC 协议被证实的。

13. 如权利要求 12 所述的方法，其特征在于，根据所述一组适用的解析参数将 DNS 查询传递到所述 DNS 服务器包括根据由所述一组适用的解析参数标识的加密技术来加密通信。

14. 如权利要求 9 所述的方法，其特征在于，所述方法还包括 ：

将所述响应和用于检索所述响应的所述一组适用的解析参数存储在高速缓存中 ；以及

在作为对所述数字标识符的第二请求的一部分接收到所述域名作为第二输入之后，确定用于检索所述响应的所述一组适用的解析参数是否足以提供对所述第二请求的响应，且如果是，则从所述高速缓存提供所述响应。

15. 如权利要求 9 所述的方法，其特征在于，所述动作 (F) 还包括 ：

(F1) 将用于所述网络资源的代理服务器的标识符提供给所述应用程序。

# 安全资源名称解析

[0001] 背景

[0002] 本发明涉及名称解析技术。在计算机通信网络中，可使用若干不同的技术来标识可经由网络访问的资源。这些资源可包括诸如客户机和服务器计算设备等附连到网络的主机，以及诸如路由器、网关、防火墙和其他设备等联网资源。在一种技术中，资源可通过诸如媒体访问控制 (MAC) 地址或网际协议 (IP) 地址等一个或多个标识号来标识。然而，已经认识到，尽管这些地址对于计算机到计算机的通信是有用的，但用户经常会发现难以记住这些标识号，且这一困难可能会阻碍用户访问网络资源。资源因此还可另外地或另选地通过更容易被用户记住的文本标识符来标识。实现用于标识资源的文本标识符的技术包括 NetBOIS、局部链路多播名称解析 (LLMNR)、以及域名系统 (DNS)。

[0003] 提供此类文本标识符的技术还可提供用于将用户容易记住的文本标识符匹配到计算机设备更容易处理的数字标识符（或相反地匹配）的转换服务。例如，在 DNS 中，当用户向计算设备输入文本标识符 (DNS 中的“域名”) 来发起与该域名所标识的资源的通信时，计算设备上的 DNS 客户端将查询 DNS 服务器来将该域名“解析”成 IP 地址。DNS 服务器在接收到查询时，将或者通过其本地可用的信息或者通过查询其他 DNS 服务器来找到对应于域名的 IP 地址，并将该 IP 地址返回给 DNS 客户端。计算设备然后可以使用该 IP 地址来发起与该资源的通信。

[0004] 已经认识到，某些这样的名称解析技术可能被滥用。例如，在 DNS 中，攻击者可能能够通过在 DNS 服务器用合法 IP 地址作出响应之前用攻击者的资源的 IP 地址响应 DNS 查询来将计算设备错误地定向到攻击者自己的资源（例如，攻击者的服务器）。计算设备因而可被错误地定向，且将连接到攻击者的资源而非合法资源。然后，在连接到攻击者的资源时，计算设备可能会向攻击者泄露数据或从攻击者接收伪造数据或恶意软件。

[0005] 已经实现了某些安全技术来例如通过在每一 DNS 查询中包括随机化标识符并要求它们被包括在对查询的响应中来降低这一情形的可能性，这将阻止攻击者用欺骗地址进行响应，除非该攻击者能够猜测出或检测到该查询的随机化标识符。已经提出来解决这些安全问题的一种安全技术是随 DNS 实现的域名系统安全扩展 (DNSSEC) 协议。DNSSEC 提供了认证机构 (CA) 对 DNS 结果进行的数字签名，使得结果可被验证为准确的。另外，已经提出了对网际协议安全 (IPsec) 协议使用 DNS 或 DNSSEC，以允许对 DNS 客户端和 DNS 服务器之间的通信进行加密和 / 或认证。

[0006] 概述

[0007] 申请人认识到并且明白包括 DNS 在内的常规名称解析技术的安全性可被改进。此外，常规名称解析技术未被设计成以经由单个网络接口和单组网络硬件连接到若干网络的方式来操作，因此阻碍了覆盖网络的增长。

[0008] 此处所描述的是用于保护名称解析技术的安全并用于确保名称解析技术能在现代网络中运作的原理。所描述的方法中的某一些与具有可经由与底层网络相同的接口访问的覆盖网络的网络配置兼容。根据此处所描述的原理中的某一些，可由诸如最终用户或管理员等用户实现一组解析参数，该组解析参数在名称解析过程中被使用来保护该过程的安

全和 / 或在覆盖网络中进行该过程。在某些实现中，该组解析参数可按照规则表来维护，并用于支配名称解析过程。例如，可创建解析参数来支配 DNSSEC 会话，或支配如何与用微软的直接访问 (Direct Access) 覆盖技术实现的网络进行通信，或支配使用任何其他联网技术的通信。

[0009] 在某些实施例中，提供提供了一种方法，该方法包括接受网络资源的第一标识符作为输入，咨询各组解析参数的集合来确定应用于第一标识符的一组适用的解析参数，以及获得第二标识符。该第二标识符可通过进行名称解析过程来基于第一标识符确定网络资源的第二标识符而获得。名称解析过程由该组适用的解析参数支配。

[0010] 在其他实施例中，提供了其上编码了计算机可执行指令的至少一个计算机可读存储介质，这些指令在被执行时使得计算机执行一种方法。该方法包括从应用程序接受可经由网络访问的资源的域名作为输入，从各组解析参数的集合中确定一组适用的解析参数，以及根据该组适用的解析参数建立到网络上的域名服务 (DNS) 服务器的连接。该 DNS 服务器可通过该组适用的解析参数来标识。该方法还包括根据该组适用的解析参数将 DNS 查询传递到 DNS 服务器，从 DNS 服务器接收包括资源的数字标识符的响应，以及将该数字标识符提供给应用程序。

[0011] 在又一些实施例中，提供了一种包括至少一个处理器和至少一个有形计算机可读存储介质的装置，该计算机可读存储介质上编码了包括与一组解析参数有关的信息的数据结构。该数据结构以可由名称解析软件组件用于支配名称解析过程的方式来存储。该数据结构包括要记录定义解析参数要应用于的网络资源的一组一个或多个标识符的信息的第一位置；要记录定义要在通信信道上实现的安全措施类型的信息的第二位置，名称解析过程要在该通信信道上交换信息；要记录定义至少一个可信证明机构的信息的第三位置；以及要记录定义要与其建立所述通信信道的至少一个网络资源的信息的第四位置。该至少一个有形计算机可读存储介质包括数据结构的多个实例，该数据结构的每一实例与一组特定的解析参数相关联。该至少一个处理器适用于执行该名称解析软件组件，且该名称解析软件组件适用于根据至少一组适用的解析参数来执行名称解析过程。该名称解析软件组件读取至少一个有形计算机可读存储介质上编码的多个数据结构中的至少某一些，以确定一组或多组适用的解析参数。

[0012] 以上概述是对由所附权利要求定义的本发明的非限定性的概述。

[0013] 附图简述

[0014] 附图不旨在按比例绘制。在附图中，各个附图中示出的每一完全相同或近乎完全相同的组件由同样的标号来表示。出于简明的目的，不是每一个组件在每张附图中均被标号。在附图中：

[0015] 图 1 示出了根据此处描述的原理中的某一些来操作的技术可在其中起作用的示例性计算机系统；

[0016] 图 2A 和 2B 示出了可根据此处所描述的原理中的某一些来实现的示例性解析参数的表；

[0017] 图 3 是可根据此处描述的原理中的某一些实现的用于执行名称解析的示例性过程的流程图；

[0018] 图 4 是可根据此处描述的原理中的某一些实现的用于标识一组适用的解析参数

的示例性过程的流程图；

[0019] 图 5 是可根据此处描述的原理中的某一些实现的用于将文本标识符解析成数字标识符的示例性过程的流程图；

[0020] 图 6 是可根据此处描述的原理中的某一些实现的用于确定存储在高速缓存中的标识符是否可作为名称解析过程的结果来返回的示例性过程的流程图；

[0021] 图 7 是可根据此处描述的原理中的某一些实现的用于确立一组解析参数的示例性过程的流程图；

[0022] 图 8 示出了可用于输入解析参数的示例性用户界面；

[0023] 图 9 是可实现根据此处描述的原理中的某一些操作的技术的示例性计算设备的组件的框图；以及

[0024] 图 10 是可依照根据本文描述的原理操作的一种或多种技术来实现的模块的互操作性的示例性方式的示图。

[0025] 详细描述

[0026] 申请人认识到并且明白包括 DNS 在内的常规名称解析技术的安全性可被改进。此外，常规名称解析技术未被设计成以经由单个网络接口和单组网络硬件连接到若干网络的方式来操作，因此阻碍了覆盖网络的增长。

[0027] 例如，尽管提出了 DNSSEC 用于确保 DNS 查询的结果是合法的，但它依赖于可能被发现是不可接受的两个条件。首先，响应 DNS 查询时所涉及的每一个 DNS 服务器（可能在不同的位置且由不同方来管理）必须被实现为处理 DNSSEC，这导致难以铺开到整个因特网。其次，DNS 客户端必须本质上担当完全解析器，而不是像普通 DNS 中那样将大多数解析查询的责任传递到完全解析器 (DNS 服务器）。这对客户端增加了处理，因为 DNS 客户端将变为负责通过检查返回给 DNS 客户端的每一结果的数字签名来确定发放用于对结果签名的证书的认证机构 (CA) 是否是应被信任的认证机构，来确保该结果是合法且正确的。将这一责任置于执行 DNS 客户端的客户计算设备上具有使计算设备负担过重的风险，这在诸如个人数字助理 (PDA) 和移动电话等能力较弱的计算设备中尤其成问题。为将这一负担从客户端去除，可将该负担置于服务器或其他网络资源上。

[0028] 此外，常规的名称解析技术不适用于在可能存在覆盖网络的情形中工作。在过去，计算设备可能通过专用网络接口来连接到每一网络，且该网络接口由用户和 / 或由每一网络上的设备来配置以便与这些网络进行交互，包括将接口配置成支持网络所实现的名称解析技术。例如，当诸如膝上型计算机等计算设备连接到有线网络时，该网络上的动态主机配置协议 (DHCP) 服务器可向计算设备提供 IP 地址、网关的标识符、以及 DNS 服务器的标识符，以及其他配置参数。使用文本标识符的通过该接口的任何通信因而将通过 DNS 服务器来解析。如果计算设备想要连接到不同网络或使用不同名称解析技术，则必须配置单独的接口。例如，可使用第二有线接口，或可使用无线接口。

[0029] 申请人认识到且明白，在现代网络中，“覆盖”网络正变得越来越常见。这些覆盖网络被配置成在相同的硬件上与现有网络共存，且是现有硬件网络之上的逻辑覆盖。连接到覆盖网络的每一网络设备也连接到一个或多个现有硬件网络，如现有局域网和 / 或现有广域网。这些覆盖网络可用各种方式中的任一种来实现，例如使用微软直接访问来实现。覆盖网络因此可被认为是一个或多个其他网络的受限子组。

[0030] 使用这些技术，连接到给定硬件网络的计算设备因此可同时经由单个接口连接到多个网络，包括底层网络和一个或多个覆盖网络。常规的名称解析技术将无法支持此类网络，因为与底层网络的名称解析技术相比，名称解析协议的类型或计算设备应与其通信来获得名称解析的网络资源（例如，DNS 服务器）对于覆盖网络可能是不同的。此外，由于某些网络可保密关于如何访问网络上的某些资源的某些信息——例如，特定安全服务器或其他网络资源的位置 / 标识——来保持该信息不被给予潜在攻击者，因此特定服务器或其他资源可能是名称解析查询的期望结果的唯一可能来源。或者，某一网络资源可具有在覆盖网络外部未知的标识符，或作为覆盖网络外部的另一资源的文本标识符的复制品的标识符，且特定服务器或其他资源可能是对于特定网络资源的名称解析查询的期望结果的唯一可能来源。因此，计算设备可能在名称解析过程期间必须联系特定服务器或其他资源，这对于覆盖网络上的通信可能与底层硬件网络不同，即使这些覆盖网络使用相同的名称解析技术。由于此原因，计算设备的一个网络接口可能必须为多个覆盖网络的每一个维护 DNS 服务器的多个地址，使得计算设备可与每一覆盖网络进行通信。这对于常规的计算设备、联网技术和名称解析技术是不可能的。

[0031] 此处所描述的是用于保证名称解析技术的安全且用于确保名称解析技术能在具有可经由单个网络接口访问的多个覆盖网络的现代网络中运作的原理。在某些实现中，诸如最终用户和 / 或管理员等用户可编译可应用于计算设备的一组解析参数以供计算设备的一个、一些或全部网络接口用于使用可通过接口访问的网络的名称解析技术来解析名称。这些解析参数然后可支配接口所执行的名称解析过程。例如，在某些这样的实现中，解析参数可指定 DNSSEC 参数和 / 或关于直接访问的参数，但应认识到可使用其他名称解析技术和其他类型的网络和安全技术。这些解析参数可用任何方式来存储，例如存储在可由名称解析模块检查并用于组成名称解析查询的规则表中。

[0032] 解析参数可包括关于如何进行名称解析过程的任何合适的信息。此外，所使用的具体参数可取决于对其寻求名称解析的网络的类型。例如，对于 DNSSEC 被用作名称解析技术的网络，这些参数可包括安全参数，如解析参数应用于哪些域、是否确认服务器证实了响应、是否应使用加密来与服务器通信、应使用什么类型的加密、应信任一个或多个什么认证来对结果签名、以及应向哪一（些）DNS 服务器查询结果。作为另一示例，对于诸如使用直接访问来实现的覆盖网络，可实现各解析参数，如解析参数应用于哪些网络 / 域、应向哪一（些）DNS 服务器查询结果、是否应使用加密、应使用什么类型的加密、应信任什么认证来对结果签名、以及在与覆盖网络通信时应使用什么代理服务器。取决于网络以及可用于实现网络的名称解析协议，可使用任何合适的解析参数。

[0033] 如此处所使用的，名称解析过程可以是用于根据任何合适的名称解析协议来确定对应于文本标识符的数字标识符或确定对应于数字标识符的文本标识符的任何合适的技术。在以下列出的示例中，域名服务 (DNS) 协议可用作名称解析协议的示例，且名称解析过程可被描述为遵守 DNS 协议。然而，应当理解，DNS 仅仅是根据此处所描述的原理操作的技术可一起操作的名称解析协议的一个示例，并且可实现任何合适的名称解析协议，本发明的各实施例在这一方面不受限制。

[0034] 应当理解，尽管此处的许多示例是在确定对应于输入文本标识符的数字标识符的上下文中描述的，但在某些实施例中，可实现另外地或另选地取数字标识符作为输入并确

定对应的文本标识符的名称解析过程。此外，应当理解，尽管以下列出的示例描述了利用文本标识符和数字标识符的一对一对应性（例如，确定对应于单个文本标识符的单个数字标识符）操作的技术，但这仅是一个示例性实施例，且在某些实现中，文本标识符可具有多个对应的数字标识符且数字标识符可具有多个对应的文本标识符。

[0035] 本文描述的技术可在各种计算系统中实现，这些计算系统的示例在下文较为详细地描述。此类系统一般涉及使用适当配置的计算设备，这些计算设备实现各自提供完成此类技术的执行所需的一个或多个操作的多个功能模块。每一个功能模块可以按照其自己的方式来实现；不必全都用相同方式实现。如此处所使用的，功能模块是执行执行操作职责的系统的结构组件。操作职责可以是整个软件元素的一部分。例如，功能模块可执行进程、离散进程、或任何其他合适的处理单元的功能。功能模块可包括计算机可执行指令，并且可在计算机存储介质上编码。此外，这样的计算机可执行指令可使用多种合适的程序设计语言和/或程序设计或脚本工具中的任何一种来编写，而且它们还可被编译为可执行机器语言代码或在框架或虚拟机上执行的中间代码。功能模块可在适当时并行或串行执行，并且可使用在其上执行这些模块的计算机上的共享存储器、使用消息传递协议、或以任何其他合适的方式，来在彼此之间传递信息。下文描述了执行一项或多项任务的示例性功能模块，但应该理解领会，所描述的功能模块和任务划分仅仅示出可实现本文描述的示例性技术的功能模块的类型，并且本发明并不限于在任何特定数量、划分、或类型的功能模块中实现。在一些实现中，所有功能可在单个功能模块中实现。此外，为清楚起见，功能模块在下文中是作为全部在一个或两个计算设备上执行来讨论的，但应该理解，在一些实现中，功能模块可在适用于彼此通信的许多分开的计算设备上实现。例如，一个计算设备可适用于执行接收诸如文本标识符等第一标识符的输入模块，并与第二计算设备上的名称解析模块进行通信来执行名称解析过程以确定对应于该文本标识符的数字标识符。

[0036] 在此处所描述的原理的一个示例性实现中，在计算设备上执行的软件应用可从用户接受所需网络资源的文本标识符的输入，其中软件应用想要与该所需网络资源建立连接。例如，软件应用可以是 web 浏览器，文本标识符可以是网站的域名，且网络资源可以是主存该网站的 web 服务器。为打开到所需网络资源的连接，软件应用或连接模块将使用网络资源的数字标识符，且因此名称解析模块（此处也称为“解析模块”）可将该文本标识符转换成用作网络地址的数字标识符，如采用 IPv4 或 IPv6 格式的 IP 地址。

[0037] 网络资源的文本标识符因此将被传递到名称解析模块，该名称解析模块适用于执行名称解析过程来获得数字标识符，名称解析模块然后可将该数字标识符返回给软件应用。然而，在执行名称解析过程之前，解析模块可审阅各组解析参数的集合来确定各组解析参数中的哪一组（如果有的话）适用于要执行的名称解析过程。该集合可用任何合适的方式来存储，包括以任何合适的格式存储在诸如存储器等计算机存储介质中。为审阅该集合来确定各组参数中的哪一组适用，解析模块可从存储器中检索该集合的一部分或全部，并执行任何种类的比较过程，包括例如将输入标识符与部分或全部组中指示特定一组解析参数适用于哪些网络资源的参数进行比较。

[0038] 该集合中的每一组解析参数可适用于一个或多个网络资源，并且可支配名称解析过程确定它们所适用的网络资源的标识符的方式。这些解析参数可包含可影响如何执行名称解析过程的任何合适的参数，包括上述示例性参数中的任一个。例如，每一组名称解析参

数可指定解析模块应与其通信来确定数字标识符的特定解析资源，如特定 DNS 服务器。

[0039] 解析模块对集合的审阅可以用任何合适的方式来完成。在一个实现中，该审阅可包括将文本标识符与各组解析参数中的每一组的标识符进行比较来确定标识符之间是否存在匹配。例如，一组解析参数的标识符可以是诸如“*.corp.contoso.com”等 DNS 后缀，使得匹配该标识符的较后部分的任何文本标识符是这些解析参数适用的标识符。由此，如果输入文本标识符是“webserver.corp.contoso.com”，则该组将是与该标识符相关联的一组参数，并且可以被认为是一组适用的解析参数。一旦确定了一组或多组适用的解析参数，就可根据适用的解析参数来进行名称解析过程。例如，如果参数指定了诸如 DNS 服务器等特定解析资源，则将建立到该解析资源的连接；如果参数指定了要使用的加密级别，则与名称解析资源的通信将使用该加密级别。

[0040] 一旦解析模块使用适用的参数建立了到解析资源的连接，就通过该连接向解析资源发出解析请求，该解析请求包括文本标识符并请求对应的数字标识符。解析资源可执行任何合适的过程，包括本领域中已知的用于确定对应的数字标识符的各种过程中的任一种，如通过咨询它本地维护的信息，或通过根据适用的解析参数将该请求转发到另一解析资源。一旦解析资源确定了数字标识符，该解析资源就可对该数字标识符执行任何合适的证实过程。例如，如果适用的解析参数指定应使用 DNSSEC 来确定数字标识符，并指定被信任来提供可用于认证结果的有效证书的一个或多个特定认证，则解析资源可在证实过程中确定结果是否是使用所述一个或多个特定认证机构中的任一个所发放的证书来签名的。如果是，则解析资源可作为解析请求的结果将数字标识符提供给计算设备上的解析模块。解析模块然后可确认该结果是根据适用的解析参数生成的，并将该结果呈现给软件应用以便在建立到所需网络资源的连接时使用。另一方面，如果该结果不是使用指定的证书签名的，则该结果可被丢弃，或随指示出它并非根据解析参数签名的指示符一起提供给解析模块。

[0041] 可通过根据此处所描述的原理执行名称解析过程来提供若干不同的优点。首先，通过维护各组解析参数的集合，名称解析过程可用解析参数来参数化以确保解析过程是安全的且结果可被信任。例如，尽管在常规名称解析技术中计算设备必须信任来自特定结果的结果是合法的，但来自该集合的解析参数允许计算设备内的解析模块查询特定的可信解析资源来以响应合法的高置信度获得所需网络资源的标识符（数字的或文本的）。此外，解析模块可以更确信指定的解析资源将具有该模块正在寻找的对应的标识符。另外，通过使用解析参数的集合，可通过指定例如是否应使用加密、应使用什么类型的加密、以及应如何证实加密来使得解析过程更安全。此外，通过指定与其进行通信的特定解析资源，该集合可使得计算设备上的解析模块能够执行更少功能且在计算设备上有更少负担，因为某些功能可被推给诸如解析资源等该集合指示为适用于进行处理的网络资源上。例如，在一个示例性 DNSSEC 实现中，某些证实过程可在网络中的诸如 DNS 服务器等解析资源上执行。解析模块在有了该集合后将知道联系能够执行 DNSSEC 任务的特定解析资源。另外，使用该集合，解析模块能够对不同的输入标识符执行不同的名称解析过程，如联系一特定解析资源来获得覆盖网络中的网络资源的文本标识符，或使用安全通信信道来交换与特定安全网络资源有关的标识符。

[0042] 根据此处所描述的原理来操作的这些和其他技术的其他功能和优点将从以下描述的示例中得到更完全的理解。以下示例旨在方便理解本发明并示出此处所描述的原理的

好处，但不例示本发明的各实施例的全部范围。

[0043] 依照本文描述的原理操作的技术可以在包括任何合适数量和类型的计算设备——包括任何合适数量和类型的网络资源——的任何合适的计算机系统中实现。图 1 示出此处描述的原理的一些示例性实现可以在其中操作的说明性计算机系统。然而，应当理解，其他实现可在任何其他合适的计算机系统中操作。

[0044] 图 1 示出包括用户设备（即计算设备 102）可以连接到的通信网络 100 的计算机系统。通信网络 100 可以是任何合适的有线和 / 或无线网络，其中包括较大有线和 / 或无线网络的一部分，诸如家庭网络、企业网的子网、因特网、和 / 或其他。计算设备 102 被示为台式个人计算机，但可以是任何合适的计算设备，诸如膝上型个人计算机、PDA、智能电话、服务器、机架式计算机、诸如路由器或交换机之类的联网设备、或其他计算设备。

[0045] 计算设备 102 耦合到存储各组解析参数的集合的数据存储 104。数据存储 104 可以在任何合适的计算机存储介质或媒体上编码，并且可用任何合适的格式来存储信息。存储在数据存储 104 中的信息中有可用于支配名称解析过程的解析参数，名称解析过程用于确定对应于输入的第一标识符的第二标识符，如确定对应于输入的文本标识符的网络资源的数字标识符。如上所述，解析参数可包括可在名称解析过程期间使用的任何合适的信息。计算设备 102 可适用于执行实现这一名称解析过程的一个或多个功能模块，在名称解析过程中，解析参数用于形成到连接到通信网络 100 的网络资源的连接。

[0046] 存储在数据存储 104 中的各组解析参数的集合可用各种方式中的任一种来供应，包括由计算设备 102 本地的用户使用任何合适的用户界面来输入，和 / 或通过由管理员使用计算设备 106 来远程供应。在一个示例中，管理员可在计算设备 106 处指定解析参数，并通过任何合适的网络管理技术将它们向下推送到计算设备 102。例如，如果通信网络 100 包括可从华盛顿州雷蒙德市的微软公司获得的微软 Windows 网络，则管理员可使用域控制器来通过活动目录 (Active Directory) 协议使用组策略将解析参数推送出去。然而，应当理解，这仅是可实现的网络管理技术的一个示例，且根据网络上可用的资源可使用任何合适的技术。

[0047] 计算设备 102 可使用各组解析参数的集合来执行用于确定诸如网络资源 108 等网络资源的标识符（数字的或文本的）的名称解析过程，该网络资源可以是诸如任何种类的服务器等可经由网络来访问的任何计算设备。为此，计算设备 102 在接受了网络资源 108 的第一标识符的输入之后，可咨询存储在数据存储 104 中的各组解析参数的集合来确定一组适用的解析参数，然后执行由该组适用的解析参数支配的名称解析过程。在名称解析过程期间，在计算设备 102 上执行的解析模块可与名称解析资源 110 通信来确定网络资源 108 的一个或多个标识符。任何合适的名称解析过程可根据此处所描述的原理来执行，包括以下描述的示例性名称解析过程的任一个。这一过程可包括以任何合适的方式与诸如解析资源 110 等任何合适的联网设备交换信息。尽管解析资源 110 在图 1 中被示为服务器，但应当理解，可使用任何合适的计算设备来作为解析资源，包括诸如个人计算机等多用途设备以及诸如硬件名称解析设备等单用途设备。

[0048] 在某些实现中，通信网络 100 可以不是单个网络，而是具有在其上被实例化的一个或多个覆盖网络 100A 的硬件网络。覆盖网络 100A 可以完全在实现通信网络 100 的硬件上被实例化，或者可以在通信网络 100 中使用的硬件上操作。通信网络 100A 可以与通信网

络 100 共享联网硬件，如路由器和交换机，但是可以存在诸如客户机和服务器计算设备等可经由硬件连接到通信网络 100 但是对于不是覆盖网络 100A 的成员的设备来说不可访问的某些网络资源。

[0049] 如上所述，为了与覆盖网络上的网络资源进行通信，计算设备 102 可能必须与具有关于覆盖网络 100A 上可用的网络资源的信息的特定解析资源进行通信，因为只有这些特定解析资源才具有关于覆盖网络 100A 上可用的网络资源的知识。在这些实现中，各组解析参数的集合可以指定一个或多个特定解析资源 110A，计算设备 102 可在名称解析过程期间与这些特定解析资源进行通信来获得诸如网络资源 108 等网络资源的标识符。该集合中的各组解析参数的某一些或全部可具有匹配覆盖网络 100A 的网络资源的标识符。当计算设备 102 的解析模块审阅该集合来确定该组适用的解析参数时，适用的解析参数可指示所需网络资源的标识符可从特定解析资源 110A 中检索。因此，计算设备 102 所执行的名称解析过程在用该组适用的解析参数参数化时，可与特定解析资源 110A 进行通信来检索所需网络资源 108 的标识符。应当理解，该审阅和名称解析过程可以用任何合适的方式来进行，包括通过以下描述的示例性技术中的任一种来进行。

[0050] 另外，在某些实现中，适用的解析参数还可指定到网络资源 108 的通信应经由代理服务器 112 来完成。在返回网络资源的第二标识符时，解析模块然后可另外地或另选地返回代理服务器 112 的标识符，如数字或文本标识符。

[0051] 如上所述，一组解析参数可包括可在进行名称解析过程时使用的任何信息。图 2A 和 2B 示出了存储在根据此处描述的原理的某些实现中可随两个示例性联网技术一起使用的各组解析参数的集合的示例性数据结构。另外，尽管图 2A 和 2B 示出了包括与两种不同技术有关的参数的两个不同集合，但应当理解，在某些实现中，这些技术可以在同一组解析参数中实现。此外，集合可被实现为任何合适的数据结构，并且在某些实现中可包括其他数据结构，每一其他数据结构存储与一组或多组解析参数有关的信息。这些数据结构可被存储在与可请求名称解析的客户计算设备相关联的计算机可读存储介质中。应当理解，图 2A 和 2B 中所示的数据结构以及它们所存储的参数仅仅是可使用的数据结构和参数的类型的图示，因为可使用任何一种或多种类型的联网技术。

[0052] 图 2A 示出了存储解析参数的集合 200A 的第一数据结构，该集合中有两组示例性解析参数。如图 2A 所示，在某些实现中，解析参数的集合可被组织为包括多个字段和行的表，每一字段指定了解析参数的类型，每一行指定了一组解析参数，但其他实现是可能的，因为可使用任何合适的格式。集合 200A 中所示的说明性解析参数包括与 DNS 解析过程有关的参数，如是否使用 DNSSEC 协议以及是否或如何实现其他 DNS 安全参数。然而，如上所述，应当理解，DNS 仅是此处描述的原理可与其一起操作的名称解析技术及协议的类型的示例，可使用任何合适的名称解析协议。

[0053] 图 2A 所示的第一说明性解析参数是“名称”参数 202。该参数 202 指示一组解析参数适用于哪些标识符，且因此该组解析参数可适用于哪一（些）网络资源。名称参数 202 可由解析模块用于确定集合中的哪一（几）组解析参数适用于对输入标识符的给定解析过程。名称参数 202 可存储网络资源的任何标识符，包括任何数字或文本标识符。例如，数字标识符可以是特定网络资源的标识符，如 IP 地址“1.2.3.4”，或可以是网络资源范围的标识符，如 IP 地址子网“157.0.0.0/8”。类似地，可用于名称参数的文本标识符可以是特定网

络资源的标识符，如像“itweb.contoso.com.”一样的完全合格域名 (FQDN)，或者可以是网络资源范围的标识符，如像“*.contoso.com”一样的 DNS 后缀或像“tweb.*”一样的 DNS 前缀。

[0054] 图 2A 所示的下一解析参数是 DNSSEC 参数 204。更具体地，示例性“DNSSEC”参数存储一二进制值（开或关），指示对于匹配名称参数的网络资源的解析过程中需要 DNSSEC 证实。当一组解析参数的 DNSSEC 参数 204 被设为开 / 真时，解析资源可根据 DNSSEC 协议来执行解析过程，并且可确保任何结果是根据解析参数被证实的。执行解析过程的解析模块还可确保 DNS 查询的任何结果已根据 DNSSEC 标准被证实，并且可例如通过在请求的首部中设置“DNSSEC OK”(DO) 标志在所发送的 DNS 请求中指示已请求了 DNSSEC 证实。

[0055] 接下来的参数与计算设备之间，例如 DNS 客户端和 DNS 服务器或任何其他设备组之间的 DNS 交换的安全性。第一个参数，即“通过 IPsec 的 DNS”参数 206 可存储指示是否在用于名称解析过程的通信信道上实现 IPsec 的二进制（开 / 关或真 / 假）值。例如，如果 IPsec 参数被设为真，则解析模块在建立到名称解析资源的连接时可以执行加密和 / 或认证过程。如果对于一组解析参数的“通过 IPSec 的 DNS”被设为开 / 真，则解析模块可检查该组的其他参数来确定用于 IPsec 协议的设置。接下来的两个参数，即“IPsec 加密级别”208 和“IPsec CA”210 是此类参数的示例。“IPsec 加密级别”可存储指定是否应使用加密和 / 或应使用什么类型的加密的任何值。“IPsec 加密级别”参数 208 可存储指示特定加密类型的无 / 低 / 中 / 高值，例如，“低”可指示任何大小的三重数据加密标准 (3DES) 或高级加密标准 (AES) 加密，而“高”可指示 192 或 256 位的 AES 加密。或者，IPsec 加密级别可存储对诸如 AES(256) 等特定加密标准的引用。“IPsec CA”210 可存储被信任来发放用于解析资源的认证证书的一个或多个证明机构的标识符。在 IPsec 的认证过程期间，当设置时，解析模块可确认解析结果是使用由可信 CA 中的一个发放给可信解析资源的认证证书来认证的。另外，如果打开了 DNSSEC，则检验来自 DNS 服务器的响应来确定响应中的扩展密钥使用 (EKU) 签名是否来自可信 CA 之一且因此确定产生该结果的 DNS 服务器被解析参数授权来代表计算设备执行 DNSSEC 证实。

[0056] 图 2A 所示的最后一个参数，即“DNS 服务器”212 可存储解析模块在解析过程期间应与其通信的一个或多个 DNS 服务器的清单。当输入到解析模块的标识符匹配一组解析参数的名称参数时，则解析模块将向“DNS 服务器”参数中列出的任何 DNS 服务器查询对应于该输入的标识符的标识符。“DNS 服务器”参数可存储可用于建立到 DNS 服务器的连接的一个或多个 DNS 服务器的任何合适的标识符，包括任何合适的数字和 / 或文本标识符。

[0057] 图 2A 示出了存储可形成集合 200A 的各组解析参数的两个说明性数据结构，每一组包括可作为该集合的参数来存储的说明性值。应当理解，这些组是可使用的组的类型的示例，并且任何值可用作参数且可使用任何数量的参数组。

[0058] 图 2B 示出了存储解析参数的集合 200B 的第二示例性数据结构。如图 2A 中一样，集合 200B 被组织为具有标识参数的多个字段和标识各组解析参数的多个行的表，但应理解，可使用任何格式。此外，在图 2B 的示例中，解析参数包括可结合用于覆盖网络的微软直接访问功能来使用的那些解析参数。然而，应当理解，直接访问仅是此处描述的原理可一起操作的联网技术和协议的类型的示例，可使用任何合适的联网技术，包括任何合适的覆盖联网技术。

[0059] 图 2B 所示的第一个参数是“名称”参数 220。类似于集合 200A 的名称参数 202，该参数标识了一组解析参数可适用的网络资源，并且可由解析模块用于确定集合中的哪一（几）组解析参数适用于对于输入的标识符的给定解析过程。名称参数 220 可存储网络资源的任何标识符，包括任何数字或文本标识符，包括以上结合集合 200A 描述的示例性参数中的任一个。

[0060] 图 2B 中的接下来的参数与直接访问技术有关。“区域专用 DNS 服务器”参数 222 可存储作为对覆盖网络上可用的网络资源的名称解析过程的一部分可被查询的一个或多个 DNS 服务器的任何合适的标识符。如上所述，在某些覆盖网络中，某些网络资源可能不能供覆盖网络所存在于的硬件网络上的所有计算设备进行一般访问，且这一限制可部分地通过不广泛地分发网络资源的标识符来实施。为获得覆盖网络上的网络资源的标识符，解析模块因而可联系一个或一小组解析资源。因此，如果输入到解析模块的标识符匹配一组解析参数的名称参数 220，则解析模块可联系“区域专用 DNS 服务器”参数 222 中指定的 DNS 服务器来获得网络资源的对应的标识符。

[0061] “区域专用代理”224 是所示的下一个参数。该参数 224 可由解析模块用于向软件应用指示该软件应用正在联系覆盖网络上的网络资源，且将软件应用配置成使用代理服务器来执行其连接或使用所标识的代理服务器来执行其连接。例如，如果软件应用期望到特定网络资源的连接且该组适用的解析参数向解析模块指示应使用代理服务器，则解析模块可向软件应用指示它应经由代理服务器来连接到网络资源。集合 200B 的代理服务器参数 224 可存储任何可接受的值，包括资源的数字和 / 或文本标识符、表示不需要代理服务器的空值或其他指示符、或指示出软件应用应使用默认代理服务器设置的值。

[0062] 下一个参数，即“通过 IPsec 的远程 DNS”226 用于指示到覆盖网络上的网络资源的连接是否应根据 IPsec 协议，如使用加密和 / 或认证来保护。如同集合 200A 的“通过 IPsec 的 DNS”参数 206 一样，集合 200B 的“通过 IPsec 的 DNS”参数 226 可采取指示是否使用 IPsec 的二进制值，如开 / 关或真 / 假。同样类似于集合 200A，“远程 DNS 加密级别”228 可存储指示在保护到解析资源的连接的安全时是否应使用加密以及使用什么类型的加密的任何合适的值，并且“IPsec CA”230 可存储被信任来发放用于解析资源的认证证书的一个或多个认证机构的任何合适的标识符。

[0063] 如同图 2A 一样，图 2B 还示出了存储可形成集合 200B 的各组解析参数的两个说明性数据结构，每一组包括可被存储在该集合的参数中的说明性值。应当理解，这些组是可使用的组的类型的示例，并且任何值可用作参数且可使用任何数量的参数组。

[0064] 此外，应当理解，尽管两个集合 200A 和 200B 被分开示出，并且着眼于两个不同技术——DNS 安全 /DNSSEC 和直接访问，但应当理解，在某些实现中，一组解析参数可包括同时针对这两种技术和 / 或针对任何其他类型的联网技术的参数。例如，对于给定覆盖网络，该组解析参数可指示解析模块使用 DNSSEC 和其他 DNS 安全措施来执行对于覆盖网络的名称解析。

[0065] 在根据此处描述的原理操作的某些技术中，可在解析参数的集合中包括另外的解析参数，但是这些另外的解析参数不是任何特定一组解析参数的一部分。这些全局参数也可用于支配解析过程，但可指示何时或是否使用各组解析参数中的任一组，可指示如何处理名称解析中的失败，或可以是适用于所有组的解析参数。例如，如果计算设备支持可以向

计算设备告知它所连接到的硬件网络的网络位置知晓 (NLA)，则该集合可包括指示基于该设备所连接到的网络的类型或身份是否要放弃对该表的全部或一部分的审阅。例如，如果 NLA 指示计算设备未连接到其上存在覆盖网络的特定硬件网络，则“NLA 绕过”参数可向解析模块指示它应当放弃审阅所有针对覆盖网络的设置，或可指示它应当放弃审阅关于特定覆盖网络的所有解析参数组。

[0066] 另外地或另选地，一全局参数可指示当位于特定网络外部时如何发出解析请求。例如，如果计算设备在特定硬件网络外部，则“查询行为”参数可指示解析模块应查询特定类型的标识符，如在 IPv4 数字标识符之前查询 IPv6 数字标识符，或仅 IPv6 数字标识符。另一全局参数可与如果名称解析过程失败则如何反应有关，这表现在未根据适用的解析参数组定位到第二标识符。该“退路行为”参数可指示解析模块应试图使用替换名称解析技术，或可指示不允许退路。例如，该参数可指示如果 DNS 过程失败，则应尝试 LLMNR 或 NetBIOS 过程。

[0067] 这些示例性集合和解析参数以及任何合适的集合中的任何其他合适的解析参数可由解析模块用于执行根据任何一种或多种类型的名称解析技术的名称解析过程。适用的解析参数组可实现并支配任何合适的名称解析过程。图 3 示出了可用于进行名称解析的过程 300。然而，应当理解，过程 300 仅是可实现的技术的类型的示例，可使用任何合适的技术。

[0068] 过程 300 在框 302 中开始，在那里计算设备的功能模块接收网络资源的第一标识符。第一标识符可由任何合适的源以及从任何合适的源接收，包括经由合适的用户界面从用户接收，包括由软件应用的用户界面接收。第一标识符可以是网络资源的任何合适的标识符，包括根据名称解析协议的任何合适的文本标识符，如 DNS 协议的域名。在框 304，然后可将第一标识符传递给名称解析模块来确定网络资源的第二标识符。这可以出于任何原因来完成。例如，如果第一标识符是软件应用接收的文本标识符，则软件应用可确定它需要网络资源的数字标识符作为第二标识符来建立到网络资源的连接。然而，这一使用情况仅是示例，因为此处描述的原理与以任何适合动机执行的名称解析过程兼容。

[0069] 在框 306，解析模块确定该集合是否具有适用于对其寻求名称解析的标识符的任何解析参数组。这可以按任何合适的方式完成。例如，解析模块可从数据存储中检索各组解析参数的集合，并将第一标识符与该集合相比较来确定各组解析参数中的哪些组（如果有的话）适用于第一标识符。该比较可以用任何方式来完成，如通过将第一标识符与以上在图 2A 和 2B 中描述的“名称”参数进行比较。解析模块然后可确定各组解析参数中的一组或多组适用于要由该模块执行的名称解析过程，并且可以或者使用该组适用的解析参数来支配该过程，或者通过以任何合适的方式合并多组解析参数来确定一组适用的解析参数。

[0070] 框 306 对一组适用的解析参数的确定可用任何合适的方式来进行。进行该步骤的确切方式可取决于该集合的格式，并取决于被选择包括在该集合中的解析参数。图 4 示出了确定过程的一个示例，但应当理解，过程 400 仅是可作为过程 300 的框 306 的一部分执行的动作的图示，且其他过程是可能的。

[0071] 过程 400 在框 402 开始，在那里解析模块从数据存储中访问各组解析参数的集合。该数据存储可以是其上执行解析模块的计算设备本地的，如图 1 的示例中那样，或者它可经由诸如计算机通信网络等任何合适的通信介质或媒体对该计算设备可用。在框 404，解

析模块可对集合中的每一组解析参数检索匹配标识符的模式，该模式指示每一组适用于网络资源的哪些标识符。该模式可以是网络资源的任何合适的指示符，包括以上结合图 2A 和 2B 描述的名称参数或任何其他数字或文本指示符。在框 406，将第一标识符与每一模式进行比较来确定对应于模式的解析参数组是否适用于第一标识符。例如，如果第一标识符是“webserver.corp.contoso.com”且模式是“*.corp.contoso.com”（其中 * 通配符），则在框 406 确定该组解析参数适用于第一标识符。

[0072] 在框 407，一旦确定了一（各）组适用的解析参数，则在所述一（各）组中检索要用于支配名称解析过程的参数。在某些实现中，将仅检索单组解析参数来作为一组适用的解析参数，而在其他实现中，可检索多组解析参数。如果获得多个组，则可使用任何合适的过程来从多组解析参数中确定适用的解析参数组。例如，可合并各参数来确定具有最高安全级别、或最低安全级别、或任何其他合适的标准的一组适用的解析参数。作为另一示例，如果多组解析参数匹配，则解析模块可选择具有最密切匹配的模式的组。例如，如果第一标识符是“a.corp.ms.com”，并且在该集合中存在对应于“corp.ms.com”的一组和对应于“ms.com”的一组，则可选择对应于“corp.ms.com”的一组解析参数，因为它更具体。

[0073] 返回到图 3 的过程 300，在框 308，一旦确定了适用的解析参数组，解析模块可执行用该组适用的解析参数参数化的名称解析过程。解析模块然后可获得网络资源的第二标识符来作为解析过程的输出。例如，如果第一标识符是文本标识符，则第二标识符可以是诸如 IP 地址等数字标识符，反之亦然。在框 310，解析模块然后可将第二标识符返回给在框 302 将第一标识符传递给它的功能模块，且该过程结束。

[0074] 框 308 和 310 的动作可用任何合适的方式来执行。图 5 示出了可用于执行用一组适用的解析参数来参数化的名称解析过程的示例性过程 500。然而，应当理解，过程 500 仅是可实现的名称解析过程的类型的图示，可根据任何合适的名称解析技术和协议来实现任何合适的过程。还应当理解，尽管过程 500 是按照特定解析参数来描述的，但这些参数也仅是示例性的，可根据此处所描述的原理使用任何合适的参数。

[0075] 图 5 的过程 500 在框 502 开始，在那里解析模块建立到由适用的解析参数组标识，如由“DNS 服务器”参数标识的名称解析资源的连接。取决于所实现的名称解析技术和协议的一个或多个类型，解析资源的特性可以变化。然而，在某些实现中，名称解析资源可以是诸如 DNS 服务器等网络资源。在框 504，根据被设为开 / 真的“通过 IPsec 的 DNS”参数，可保护到解析资源的连接。连接的安全性可取决于其他参数，如标识要使用的加密的类型的“加密级别”参数和 / 或标识可发放认证解析资源的身份的证书的一个或多个认证机构的“IPsec CA”参数。用于保护使用 IPsec 协议的通信连接的技术在本领域中是公知的，且将不在此处更详细地讨论。

[0076] 在框 506，一旦保护了到解析资源的连接，解析模块可通过信道来传递名称解析请求。解析请求可包括用于执行名称解析的任何合适的数据，包括第一标识符和指示解析资源可能需要遵循的过程的任何参数。例如，根据适用的解析参数组的某一参数，解析请求可指示对解析请求已启用 DNSSEC，并且解析资源应在返回第二标识符之前根据 DNSSEC 对第二标识符执行证实过程。例如，该解析请求可包括该组解析参数指示出的被信任来返回可信结果的一个或多个认证机构的一个或多个指示符，解析资源可确认使用了这些认证机构中的一个。

[0077] 根据所选择且由解析参数指示的具体名称解析技术，解析资源可进行任何合适的技术来获得网络资源的第二标识符。例如，如果解析资源是 DNS 服务器，则解析资源可检查其本地的标识符高速缓存来确定它是否“知道”对应于解析请求中所接收的第一标识符的第二标识符。如果第二标识符不在其高速缓存中，则它可将解析请求传送到另一 DNS 服务器，该另一 DNS 服务器然后可进行相同的过程。这将继续直到原始解析资源接收到包括第二标识符的响应。如果该组适用的解析参数指示 DNSSEC 为“开”，则当解析资源或者从其自己的高速缓存或者从另一 DNS 服务器获得结果时，解析资源可检查该结果来确定它是否已由可保证结果的合法性的可信源“签名”。如果结果被确定为是有效的，则它可被返回给发出了解析请求的解析模块。

[0078] 在框 508，解析模块通过安全信道从解析资源接收响应，且在框 510，确认第二标识符由解析资源证实且由可信的认证机构签名。在框 512，基于框 510 的确定，解析模块确定该标识符是否根据该组适用的解析参数被证实。如果第二标识符被证实，则在框 514，将第二标识符返回给最初通过提供第一标识符而发出请求的功能模块（如在图 3 的框 302 中），且该过程结束。另一方面，如果响应未根据该组适用的解析参数被证实，则在框 516，解析模块处理掉该结果并向功能模块返回指示未找到结果的错误消息，且该过程结束。

[0079] 在某些实现中，解析模块还可维护网络资源的标识符的本地高速存储。解析模块在接收到包含第二标识符的对解析请求的响应时，可在高速缓存中存储第一标识符、第二标识符和用于获得第二标识符的解析参数。然后，当解析模块接收到对第二标识符的新请求时，解析模块可检查高速缓存来确定它是否已经存储了第二标识符，且如果是，则可从高速缓存返回第二标识符而不向解析资源发出解析请求。图 6 示出了用于使用高速缓存来执行解析过程的示例性过程 600。然而，应当理解，过程 600 仅是说明性的，且可根据此处所描述的原理实现任何合适的技术。

[0080] 过程 600 在框 602 开始，在那里解析模块接收第一标识符并确定一组适用的解析参数。这可用任何合适的方式来完成，包括通过上述示例性技术中的任一种。在框 604，解析模块可检查高速缓存来确定第一标识符是否在高速缓存中被列出。如果基于框 606 的判定，第一标识符不在高速缓存中，则在框 608 名称解析过程如上所述地继续。当通过名称解析过程获得了第二标识符时，则在框 610 可将描述该获得动作的信息存储在高速缓存中。该信息可包括关于获得过程的各种类型的数据和指令中的任一种。例如，该信息可包括第一标识符、第二标识符和 / 或在获得动作中使用的该组适用的解析参数。一旦将信息存储在高速缓存中，过程 600 结束。

[0081] 另一方面，如果在框 606 确定第一标识符在高速缓存中，则在框 612，检索与第一标识符一起存储在高速缓存中的该组解析参数并将其与在框 602 中检索出的一组适用的解析参数进行比较。可以完成该比较来确保从高速缓存返回的任何第二标识符是根据该组适用的解析参数获得的标识符。例如，框 612 的比较可确定参数是相等的，或者用于获得存储在高速缓存中的标识符的参数至少与框 602 中检索出的参数一样安全。或者，框 612 的比较可确定高速缓存中的第二标识符的源——从中获得第二标识符的解析资源——与该组适用的解析参数所需的源相同。作为另一示例，高速缓存可改为存储检索到第二标识符的时间，且解析模块可将其与编辑解析参数的最后时间进行比较来确定解析参数在执行时与在检索高速缓存中的标识符时是否是相同的。在框 612 可进行任何合适的比较过程。

[0082] 在框 614，如果参数不匹配，则如上所述根据该组适用的解析参数来进行名称解析过程，以确保所获得的任何标识符是适当地获得的。然而，如果在框 614 确定参数匹配，则在框 616，从高速缓存返回第二标识符到提供第一参数的功能模块，且过程 600 结束。

[0083] 上述的是用于基于功能模块输入到解析模块的第一标识符来确定第二标识符的若干不同的技术。然而，应当理解，这些技术中的每一种都仅是可根据此处所描述的原理实现的技术的类型的图示。可实现任何一种或多种类型的方法来进行名称解析过程以基于名称解析技术确定网络资源的标识符，不论被实现为硬件网络还是覆盖网络，或者可基于为解析模块供应的解析参数来确定网络资源的标识符。

[0084] 为解析模块供应的解析参数可用任何合适的方式来供应。例如，在一个实现中，解析参数可由计算设备的用户本地输入，并存储在与计算设备相关联的数据存储中。在另一实现中，解析参数可在计算设备连接到网络时通过网络来提供。图 7 示出了用于经由网络向计算设备提供解析参数的一个这样的后一过程的示例。然而，应当理解，图 7 的过程 700 仅是说明性的，且其他过程是可能的。此外，应当理解，尽管图 7 的示例是按照微软 Windows 计算机网络来描述的，但其他网络也是可能的，在这些其他网络中，计算设备在连接到网络时由网络来配置。

[0085] 过程 700 在框 702 开始，在那里管理员将解析参数的集合输入到网络的域控制器中。该解析参数的集合可以用任何合适的方式来输入，包括作为用于网络的微软活动目录组策略的一部分来输入。组策略可应用于网络的任何部分，包括应用于连接到网络的一组计算设备和 / 或应用于网络的一组用户。在框 704，域控制器接收解析参数并将其作为组策略来存储，然后将组策略发送到该组的所有成员。框 704 的该发送可在诸如每 15 秒等一设定时间段之后进行，或在组的成员（或是计算机或是用户）加入或登录到网络时进行。在框 706，执行此处所描述的解析模块的计算设备以任何合适的方式接收组策略并将其存储在与计算设备相关联的数据存储中。然后，在框 708，当执行名称解析过程时，解析模块以任何合适的方式，包括上述示例性技术中的任一种，将解析模块的集合应用于名称解析过程。

[0086] 可使用任何合适的用户界面来输入解析参数。例如，在某些实现中，可使用基于文本的命令行工具来输入解析参数。在其他实现中，可使用图形用户界面来输入解析参数。图 8 示出了可根据此处描述的原理中的某一些来使用的一个这样的图形用户界面的示例。然而，应当理解，某些实现可使用替换的用户界面，本发明的各实施例不限于对解析参数使用任何特定的输入技术。

[0087] 图形用户界面 800 包括可用于输入解析参数的多个控件。可使用文本框 802 来输入网络资源的名称，包括要用于匹配网络资源的名称的模式，如在以上结合图 2A 和 2B 描述的“名称”参数中。该图形用户界面还可包括输入与认证机构有关的信息，该认证机构可用于 IPsec 安全过程和 / 或用于根据像 DNSSEC 之类的安全名称解析技术来对标识符签名。也可实现与 DNS 安全有关的一系列控件 806，具有指示如是否需要 DNSSEC 证实、是否使用 IPsec、以及如果使用 IPsec 则使用什么类型的加密等参数的控件。也可实现另一系列控件 808 来用于诸如直接访问等覆盖网络，接受各参数，如诸如 DNS 服务器等可接受的解析资源的标识符、要使用的代理服务器的标识符、是否使用 IPsec、以及如果要实现 IPsec 则使用什么类型的加密。图形用户界面 800 还包括用于创建并更新一组解析参数的按钮 810，这些参数包括在控件 802-808 中的每一个中输入的参数。其他全局解析参数也可经由框架 812

输入到该图形界面。一旦创建了一组解析参数，则可将该组参数显示在图形用户界面 800 底部的框架 814 中，该框架具有对齐到可使用界面 800 输入的参数的类型的多个列。

[0088] 当使用图形用户界面 800 创建或更新了一组参数时，该组参数可用任何合适的格式存储在任何合适的数据结构中。该数据结构可被存储在存储各组解析参数的集合，如图 2A 和 2B 的集合 200A 和 200B 的数据结构中。如上所讨论的，这些数据结构可被编码在任何合适的计算机存储介质上。因此，当用户使用图形用户界面 800 来输入参数时，图形用户界面 800 可发起一记录过程来以任何合适的方式将输入参数记录到计算机可读介质上。

[0089] 根据本文描述的一些或所有原理操作的技术可以按任何方式实现。例如，在一些实现中，这些技术可被实现为在一个或多个计算机可读存储介质上编码的计算机可执行指令，这些计算机可读存储介质诸如有磁介质（例如，硬盘驱动器）、紧致盘 (CD)、数字多功能盘 (DVD)、持久或非持久固态存储器（例如，闪存、磁 RAM 等）、或任何其他合适的存储介质。计算机存储介质可被实现为图 9 的计算机可读存储介质 906（即，作为计算设备 900 的一部分）或被实现为单独的计算机存储介质。应当理解，如此处所使用的，包括“计算机可读存储介质”的“计算机可读介质”指的是具有可在其上记录数据的过程期间用某种方式更改的至少一个物理结构的有形存储介质。例如，计算机可读介质的物理结构的一部分的磁化状态可在记录过程中更改。

[0090] 在一些此类实施例中，实现依照本文描述的原理来操作的技术的计算机可执行指令可被实现为一个或多个独立功能模块（例如，如上所述的解析模块）。如上所述，“功能模块”是系统中执行特定操作角色的结构组件，然而在实例化后，功能模块可以是整个软件元素的一部分或整个软件元素（例如，功能或离散进程）。一般而言，功能模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等。通常，在各实施例中，功能模块的功能可以视需要组合或分布。这些功能模块在一些实现中可适于与其他不相关的功能模块和 / 或过程交互，诸如实现软件程序应用或实现计算设备的操作系统的模块，或者在其他实现中，这些模块可适于与其他功能模块交互，这些其他功能模块与这些模块一起构成诸如操作系统之类的整体系统，诸如可从华盛顿州雷蒙德市的微软公司购买到的微软 Windows 操作系统（即，这些功能模块可被实现为操作系统的一部分或在操作系统的外部实现）。还应当理解，在某些实现中，某些功能模块可与其他功能模块分开实现，或可以不实现某些功能模块。

[0091] 在一些但并非全部实现中，这些技术可体现为可在包括图 1 的示例性计算机系统的任何合适计算机系统中操作的任何合适计算设备上执行的计算机可执行指令。例如，根据本文讨论的一些或所有原理来操作的技术可以在以下系统上操作：单个多用途可编程数字计算机装置、共享处理能力并联合执行本文描述的技术的两个或更多多用途计算机装置的协调系统、专用于执行本文描述的技术的单个计算机装置或计算机装置（同处一处或在地理上分布）的协调系统、用于执行本文描述的技术的一个或多个专用集成电路 (ASIC)、用于执行本文描述的技术的一个或多个现场可编程门阵列 (FPGA)、或任何其他合适的系统。

[0092] 图 9 示出了计算设备 900 形式的可用于实现本文描述的技术的系统中的计算设备的一个示例性实现，然而其他实现也是可能的。此外，应理解，图 9 既不旨在是对用于依照本发明描述的原理操作的计算设备的必要组件的描绘，也不旨在是全面描绘。

[0093] 计算设备 900 可包括处理器 902、网络适配器 904、以及计算机可读存储介质 906。计算设备 900 可以是例如台式或膝上型个人计算机、工作站、服务器、大型机、智能电话、或任何其他合适的计算设备。网络适配器 904 可以是使得计算设备 900 能够通过任何合适的计算网络来与任何其他合适的计算设备进行通信的任何合适的硬件和 / 或软件。该计算网络可以是用于在两个或更多个计算机之间交换数据的任何合适的一个或多个有线和 / 或无线通信介质，包括因特网。在一些实现中，网络适配器 904 可被实现为两个或更多单独的网络适配器，以提供经由两种或更多种类型的接口的连接（例如，诸如以太网适配器之类的有线网络适配器和诸如 IEEE 802.11g 适配器之类的无线网络适配器）。计算机可读存储介质 906 可以是适用于存储要由处理器 902 处理的数据和 / 或要由处理器 902 执行的指令的任何合适的有形存储介质。处理器 902 能够处理数据和执行指令。这些数据和指令可被存储在计算机可读存储介质 906 上，并且例如可以启用计算设备 900 的各组件之间的通信。

[0094] 存储在计算机可读存储介质 906 上的数据和指令可包括实现根据本文描述的原理操作的技术的计算机可执行指令。在图 9 的示例中，如上所述，计算机可读存储介质 906 存储实现各种模块并存储各种信息的计算机可执行指令。计算机可读存储介质 906 存储与可在计算设备上执行的一个或多个应用程序 908 有关的数据和指令。这些应用程序可包括可接受网络资源的第一标识符并试图获得该网络资源的第二标识符的应用程序。计算机可读存储介质 906 还可包括用于基于第一标识符根据包括上述示例性技术中的任一种的任何合适的技术来确定网络资源的第二标识符的名称解析模块 910。计算机可读存储介质 906 还包括各组解析参数的集合 912。如上所讨论的，该集合可用任何合适的方式来组织和格式化，并且解析参数可包括用于支配名称解析模块 910 的名称解析过程的执行的任何合适的参数。在一个实现中，例如，集合 912 可以在计算机可读存储介质 906 上作为微软 Windows 操作系统的注册表的一部分来实现。计算机可读存储介质 906 另外可包括已经由名称解析模块 910 检索的标识符的高速缓存 914。该高速缓存可以用任何合适的方式来组织，并且可包含任何合适的一种或多种类型的信息，包括网络资源的各组第一和第二标识符、用于获得标识符的各组解析参数、获得标识符的时间、和 / 或任何其他一种或多种类型的信息。

[0095] 最后，在图 9 的示例中，计算机可读存储介质 906 可以包括实现各组解析参数的集合并确定该集合的内容的一组应用程序编程接口 (API) 函数。例如，该 API 可实现 GetProxyInfo（获得代理信息）函数来确定可用于联系特定网络资源、取得网络资源的标识符作为输入的代理。GetProxyInfo 函数可使用资源的输入标识符来定位集合中适用于该网络资源的一组或多组解析参数，然后可在各组解析参数中的任一组指示要使用代理服务器时返回代理服务器的标识符。也可实现 GetPolicyTableInfo（获得策略表信息）API 函数来返回集合的内容（即，各组解析参数）。此外，GetEffectivePolicy（获得有效策略）API 函数可取决于哪些解析参数不适用于给定情形来返回集合中的部分（或全部）各组解析参数。例如，如果各组解析参数中的某一些适用于特定网络且计算设备 900 未连接到该网络，则这些组可以不作为 GetEffectivePolicy 函数的输出的一部分来返回。另外，可实现取第一参数作为输入并执行由各组解析参数的集合支配的名称解析过程来确定第二标识符并返回第二标识符的 GetAddrInfo（获得地址信息）或 DnsQuery(DNS 查询）函数。应当理解，这些 API 函数仅是可实现的 API 函数的类型的示例，本发明的各实施例在这一方面

不受限制。

[0096] 实现根据本文描述的原理操作的技术的模块可以按任何合适方式交互。图 10 示出可根据本文描述的一些原理实现的模块的一种示例性安排。

[0097] 在图 10 的示例中，应用程序 1000 与连接模块 1002 和名称解析模块 1004 中的一个或两者进行交互来确定对应于第一标识符的第二标识符。例如，应用程序 1000 可直接查询名称解析模块 1004，或者应用程序 1000 可试图使用第一标识符利用连接模块 1002 来打开到网络资源的连接，并且该连接模块可向名称解析模块请求第二标识符以便在打开连接时使用。名称解析模块 1004 在尝试获得第二标识符时可如上所述使用各组解析参数的集合 1006，并且还可如上所述地使用标识符的高速缓存 1008。最后，在使用解析参数的集合 1006 来获得第二标识符时，名称解析模块 1004 还可使用各种连接技术 1010，包括使用连接模块 1012 来打开到解析资源的连接，以及使用认证模块 1014 和 / 或加密模块 1016 来执行可由集合中的解析参数规定的任何安全过程。

[0098] 至此描述了本发明的至少一个实施例的若干方面，可以理解，本领域的技术人员可容易地想到各种更改、修改和改进。

[0099] 这样的更改、修改和改进旨在是本发明的一部分，且旨在处于本发明的精神和范围内。因此，上述描述和附图仅用作示例。

[0100] 本发明的各个方面可单独、组合或以未在前述实施例中具体讨论的各种安排来使用，从而并不将其应用限于前述描述中所述或附图中所示的组件的细节和安排。例如，可使用任何方式将一个实施例中描述的各方面与其他实施例中描述的各方面组合。

[0101] 同样，本发明可被具体化为方法，其示例已经提供。作为该方法的一部分所执行的动作可以按任何合适的方式来排序。因此，可以构建各个实施例，其中各动作以与所示的次序所不同的次序执行，不同的次序可包括同时执行某些动作，即使这些动作在各说明性实施例中被示为顺序动作。

[0102] 在权利要求书中使用诸如“第一”、“第二”、“第三”等序数词来修饰权利要求元素本身并不意味着一个权利要求元素较之另一个权利要求元素的优先级、先后次序或顺序、或者方法的各动作执行的时间顺序，而仅用作将具有某一名字的一个权利要求元素与（若不是使用序数词则）具有同一名字的另一元素区分开的标签以区分各权利要求元素。

[0103] 同样，此处所使用的短语和术语是出于描述的目的而不应被认为是限制。此处对“包括”、“包含”、“具有”、“含有”、“涉及”及其变型的使用旨在包括其后所列的项目及其等效物以及其他项目。

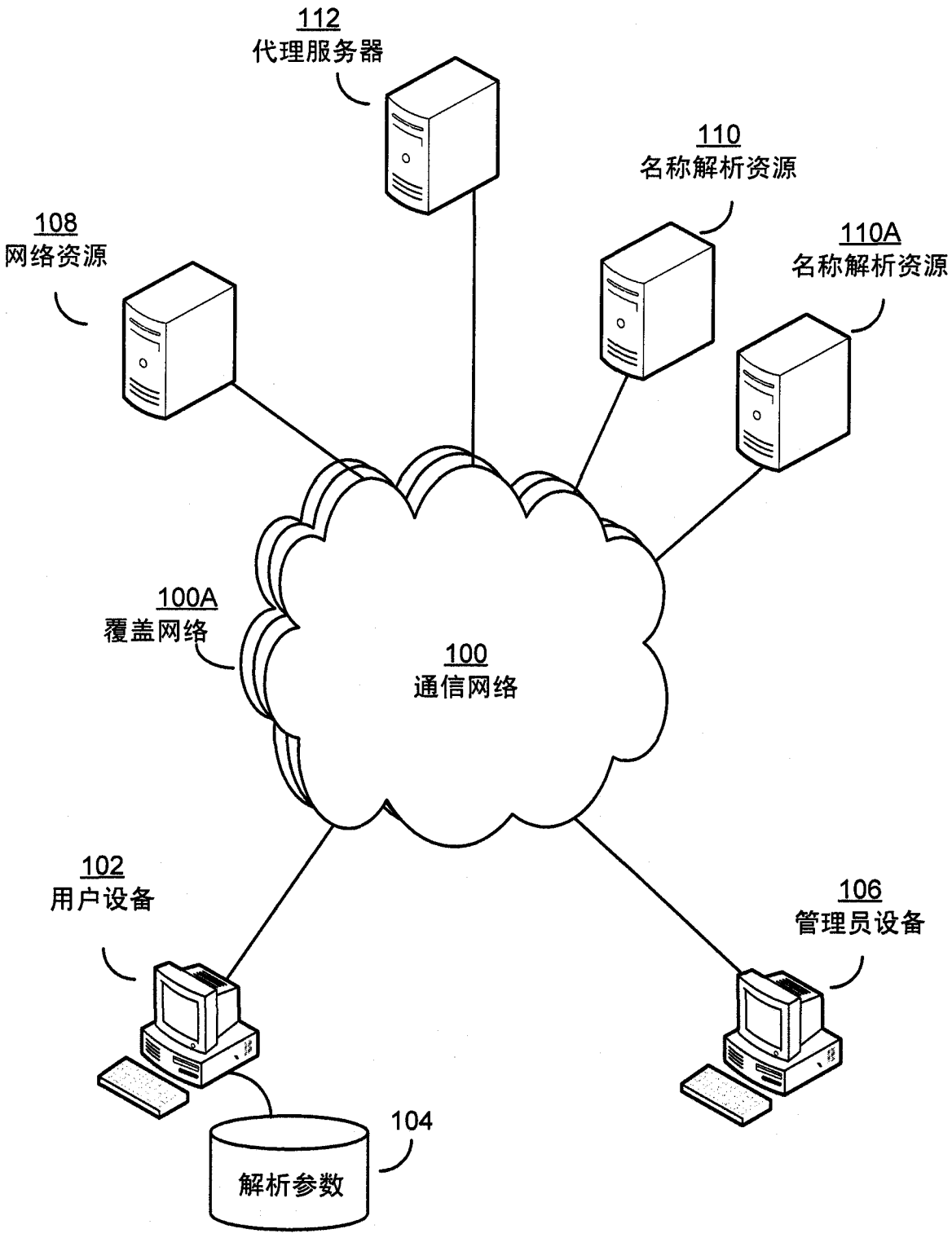

112
代理服务器
110
名称解析资源
108
网络资源
110A
名称解析资源
100A
覆盖网络
100
通信网络
102
用户设备
106
管理员设备
104
解析参数

图 1

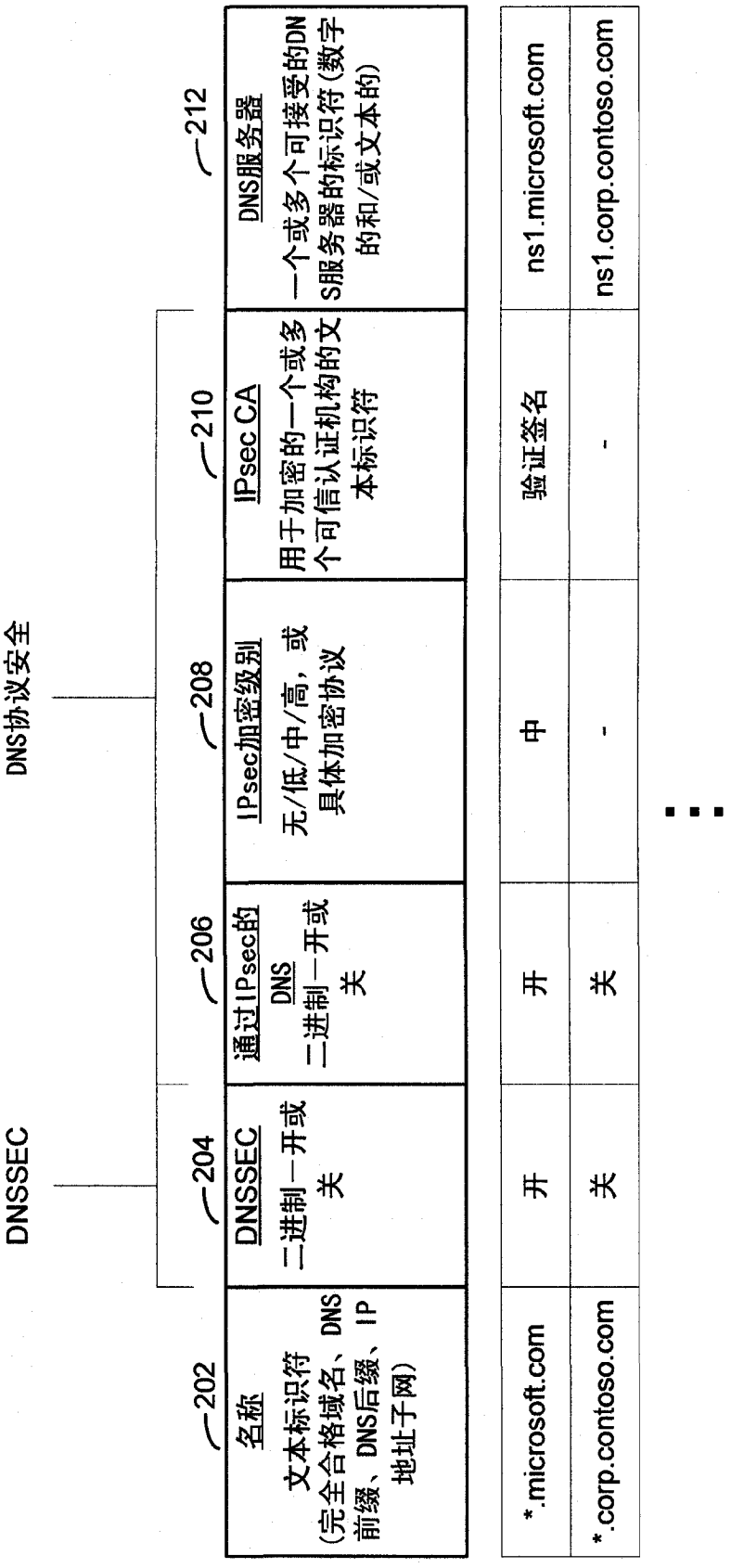

200A
DNS协议安全
DNSSEC
202
名称
文本标识符（完全合格域名、DNS前缀、DNS后缀、IP地址子网）
204
DNSSEC
二进制—开或关
206
通过IPsec的DNS
二进制—开或关
208
IPsec加密级别
无/低/中/高，或具体加密协议
210
IPsec CA
用于加密的一个或多个可信认证机构的文本标识符
212
DNS服务器
一个或多个可接受的DNS服务器的标识符（数字的和/或文本的）
*.microsoft.com
开
开
中
验证签名
ns1.microsoft.com
*.corp.contoso.com
关
关
-
-
ns1.corp.contoso.com

图 2A

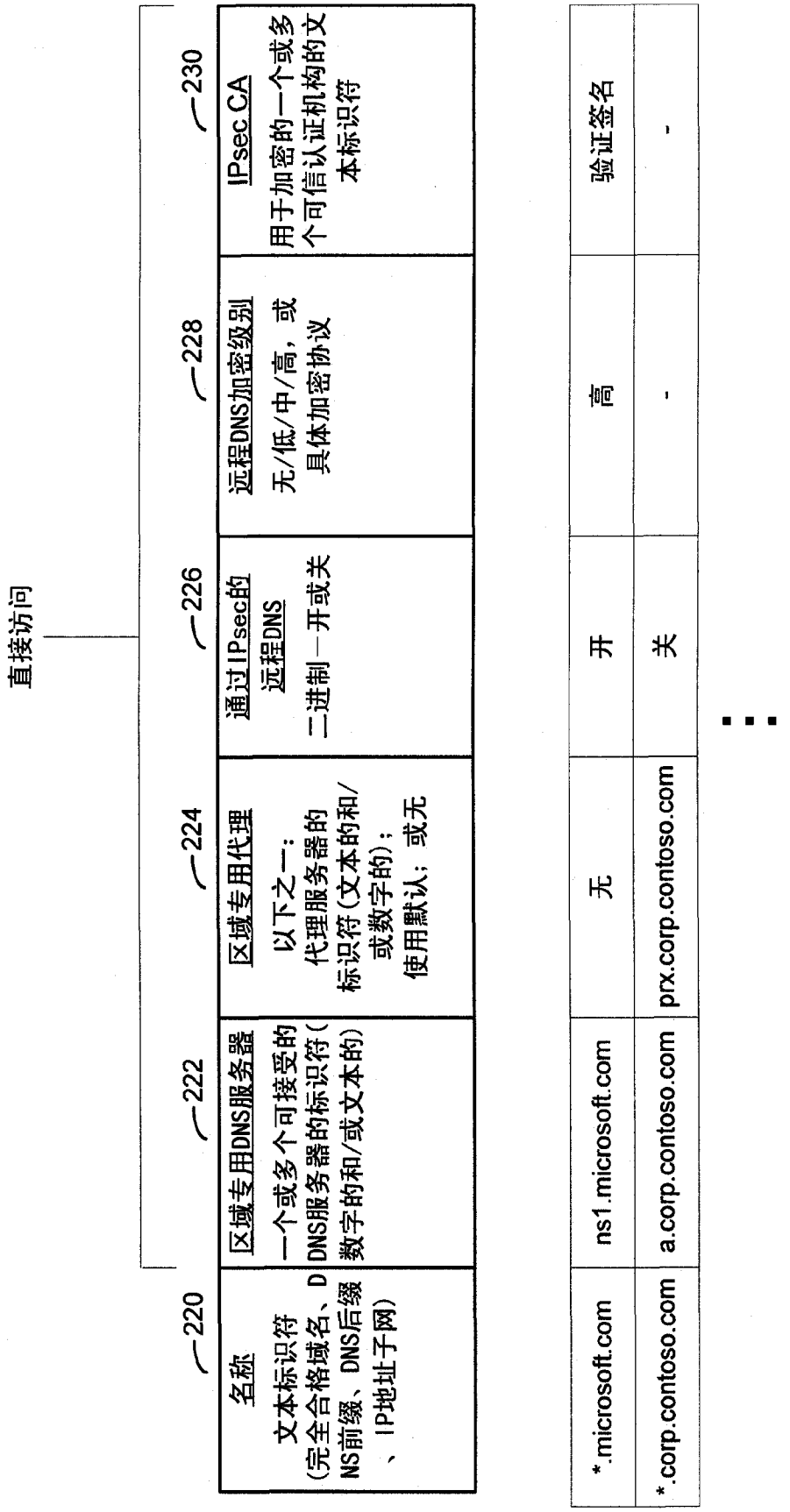

200B
直接访问
220
222
224
226
228
230
名称
文本标识符
(完全合格域名、DNS前缀、DNS后缀、IP地址子网)
区域专用DNS服务器
一个或多个可接受的DNS服务器的标识符(数字的和/或文本的)
区域专用代理
以下之一:
代理服务器的标识符(文本的和/或数字的);
使用默认;或无
通过IPsec的远程DNS
二进制—开或关
远程DNS加密级别
无/低/中/高,或具体加密协议
IPsec CA
用于加密的一个或多个可信认证机构的文本标识符
*.microsoft.com
ns1.microsoft.com
无
开
高
-
*.corp.contoso.com
a.corp.contoso.com
prx.corp.contoso.com
关
-
-
验证签名

图 2B

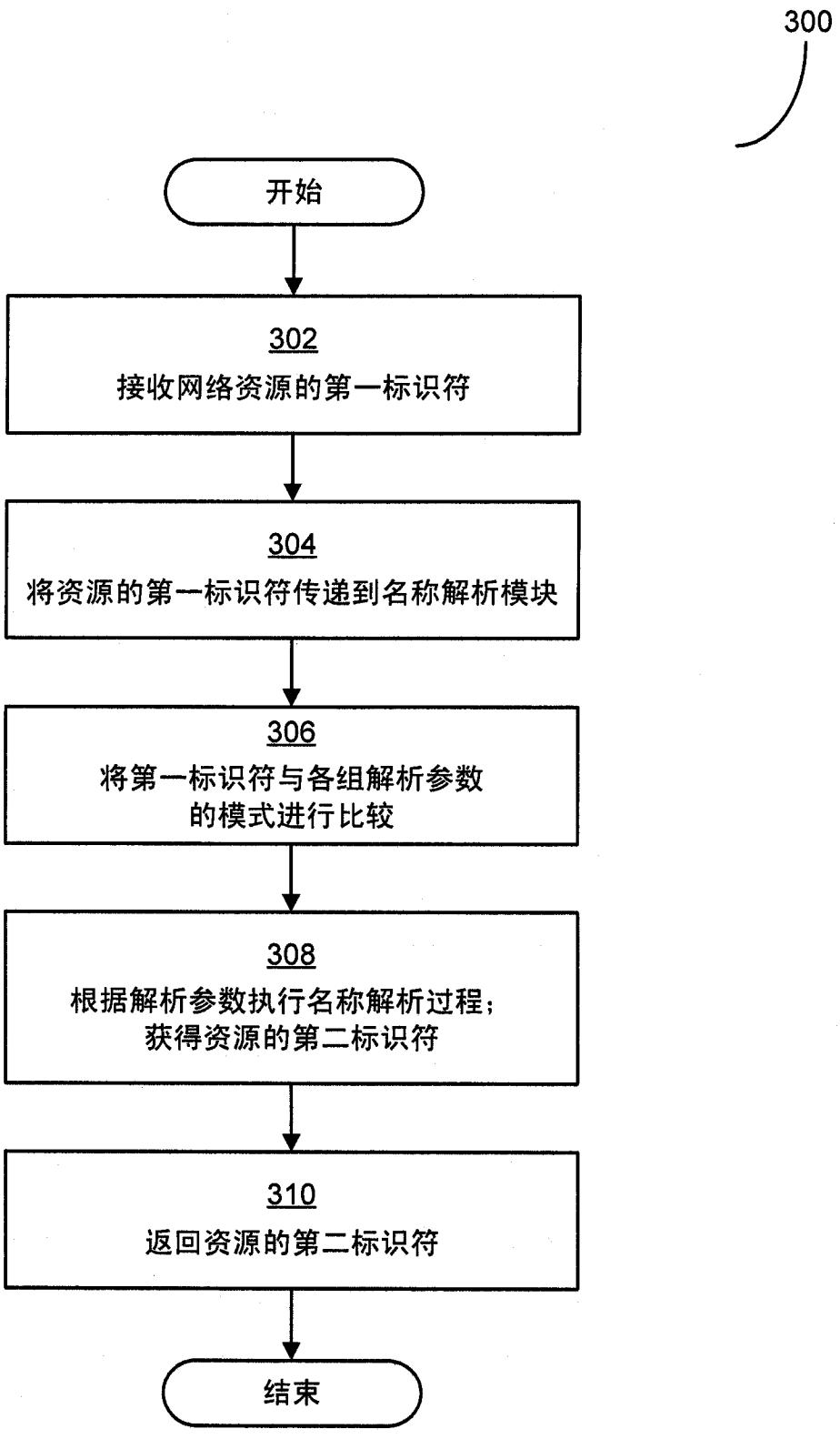

300
开始
302
接收网络资源的第一标识符
304
将资源的第一标识符传递到名称解析模块
306
将第一标识符与各组解析参数的模式进行比较
308
根据解析参数执行名称解析过程；获得资源的第二标识符
310
返回资源的第二标识符
结束

图 3

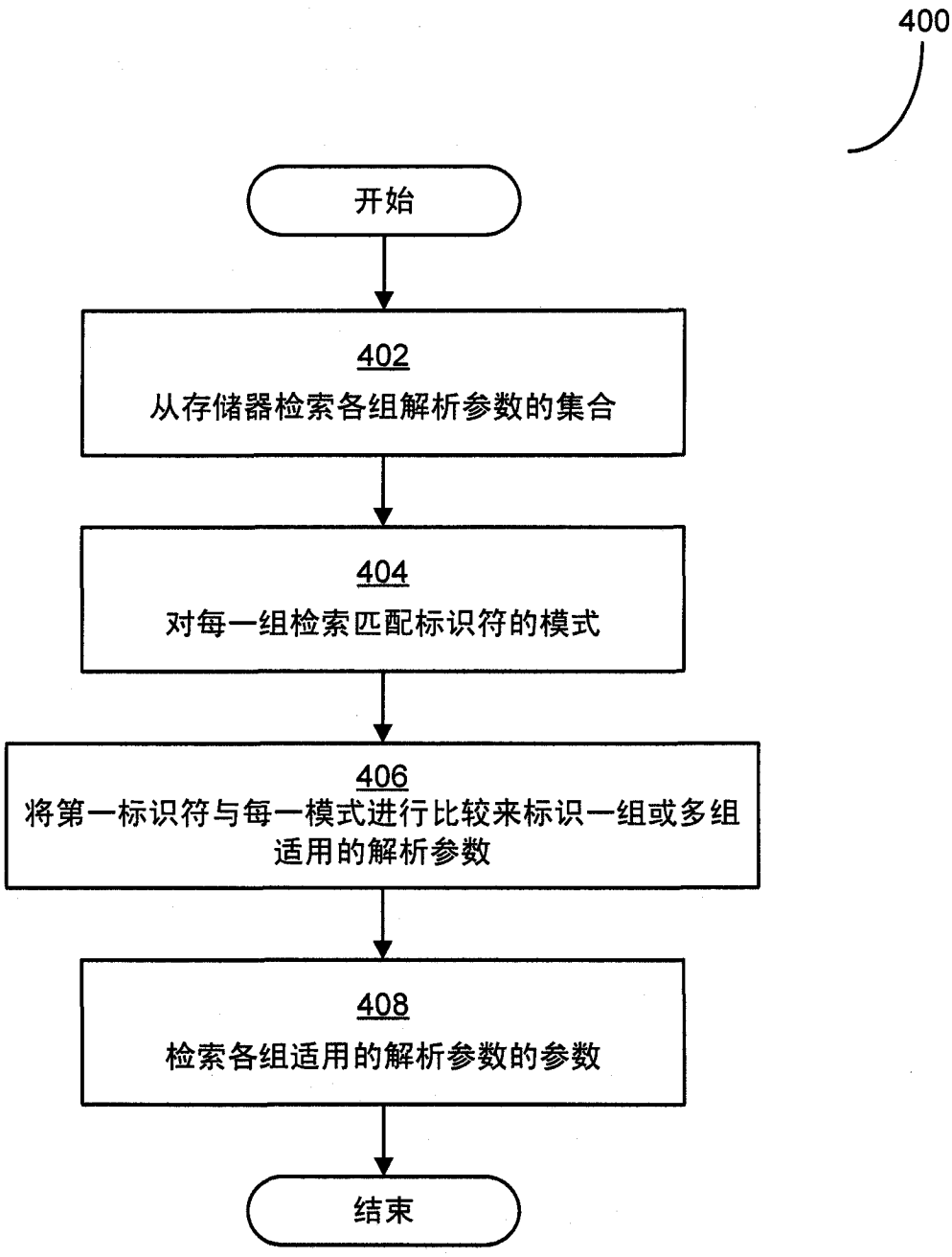

400
开始
402
从存储器检索各组解析参数的集合
404
对每一组检索匹配标识符的模式
406
将第一标识符与每一模式进行比较来标识一组或多组适用的解析参数
408
检索各组适用的解析参数的参数
结束

图 4

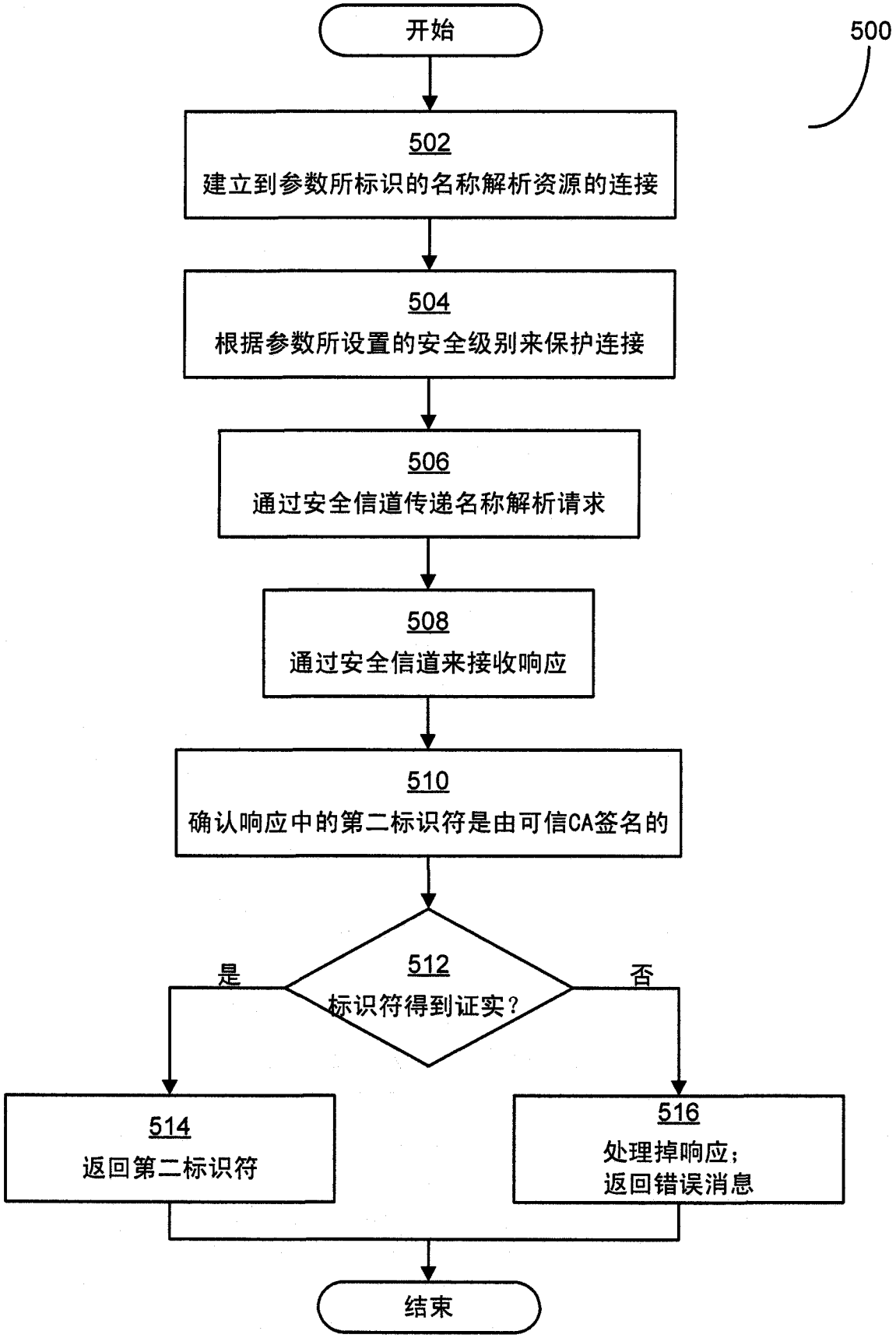

开始
500
502
建立到参数所标识的名称解析资源的连接
504
根据参数所设置的安全级别来保护连接
506
通过安全信道传递名称解析请求
508
通过安全信道来接收响应
510
确认响应中的第二标识符是由可信CA签名的
512
标识符得到证实？
是
否
514
返回第二标识符
516
处理掉响应；
返回错误消息
结束

图 5

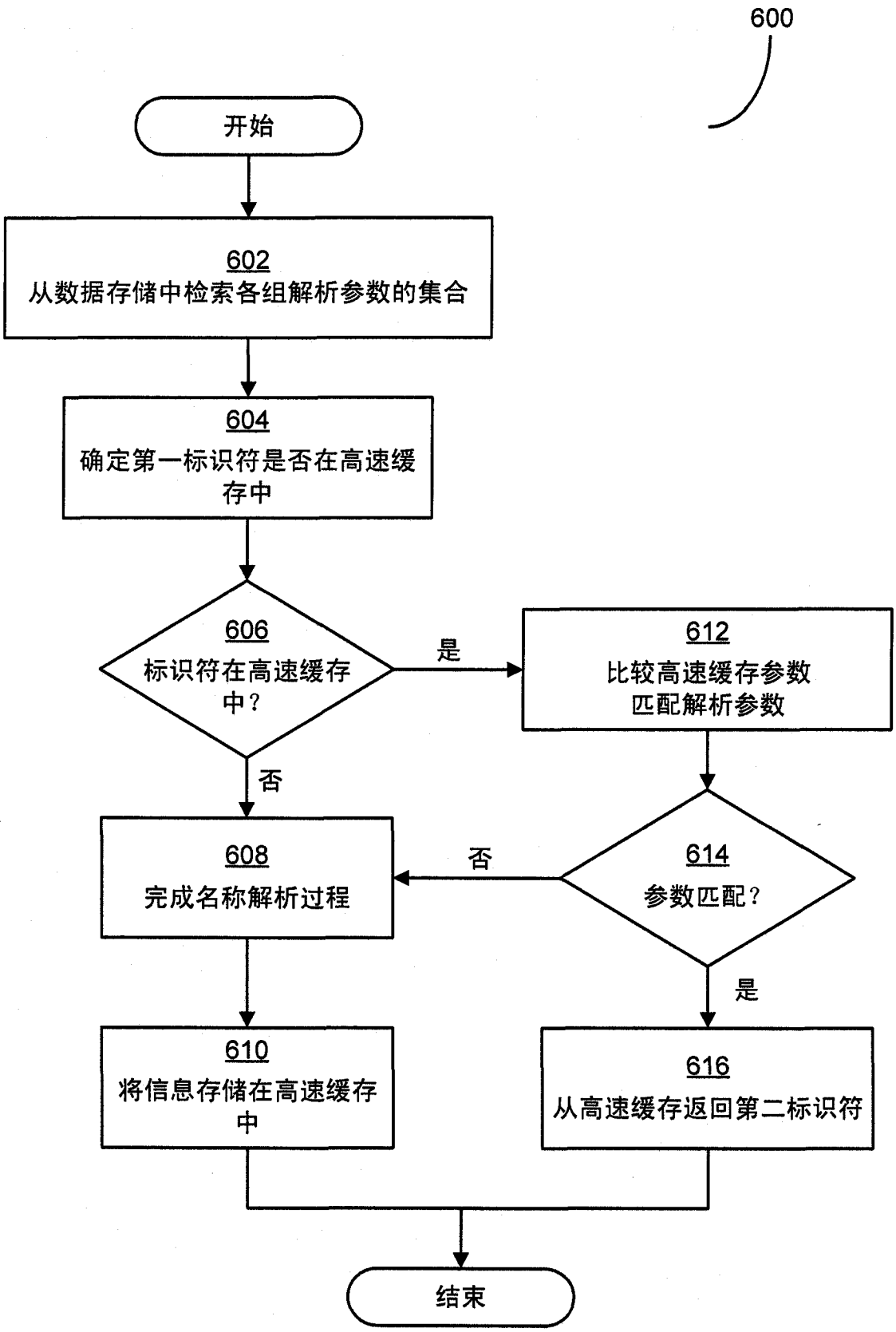

600
开始
602
从数据存储中检索各组解析参数的集合
604
确定第一标识符是否在高速缓存中
606
标识符在高速缓存中？
是
否
612
比较高速缓存参数匹配解析参数
614
参数匹配？
否
是
608
完成名称解析过程
610
将信息存储在高速缓存中
616
从高速缓存返回第二标识符
结束

图 6

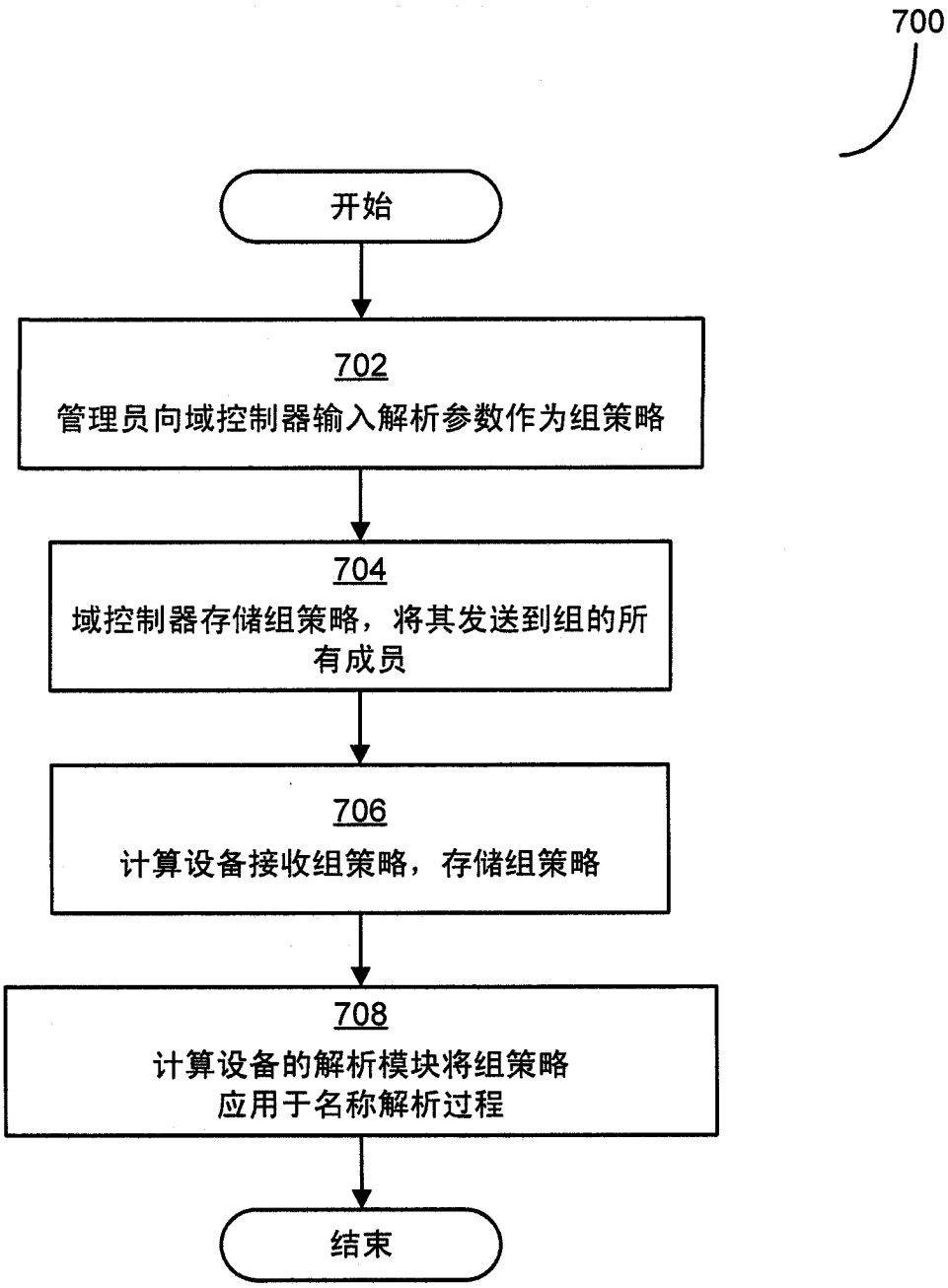

700
开始
702
管理员向域控制器输入解析参数作为组策略
704
域控制器存储组策略，将其发送到组的所有成员
706
计算设备接收组策略，存储组策略
708
计算设备的解析模块将组策略应用于名称解析过程
结束

图 7

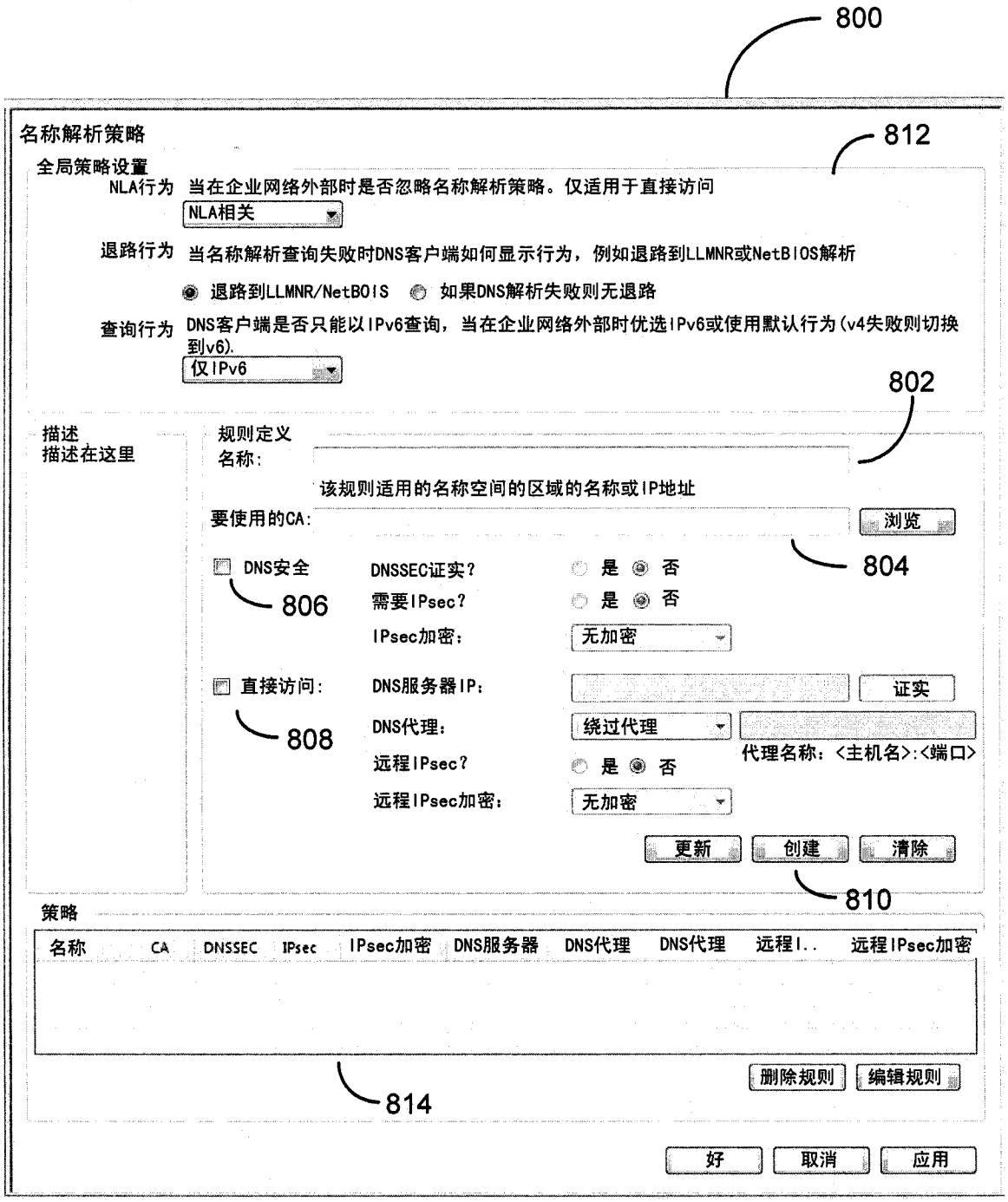

800
名称解析策略
812
全局策略设置
NLA行为
当在企业网络外部时是否忽略名称解析策略。仅适用于直接访问
NLA相关
退路行为
当名称解析查询失败时DNS客户端如何显示行为，例如退路到LLMNR或NetBIOS解析
退路到LLMNR/NetBOIS
如果DNS解析失败则无退路
查询行为
DNS客户端是否只能以IPv6查询，当在企业网络外部时优选IPv6或使用默认行为(v4失败则切换到v6).
仅IPv6
802
描述
描述在这里
规则定义
名称:
该规则适用的名称空间的区域的名称或IP地址
要使用的CA:
浏览
804
DNS安全
806
DNSSEC证实?
是
否
需要IPsec?
是
否
IPsec加密:
无加密
直接访问:
808
DNS服务器IP:
证实
DNS代理:
绕过代理
代理名称：<主机名>:<端口>
远程IPsec?
是
否
远程IPsec加密:
无加密
更新
创建
清除
810
策略
名称
CA
DNSSEC
IPsec
IPsec加密
DNS服务器
DNS代理
DNS代理
远程I..
远程IPsec加密
删除规则
编辑规则
814
好
取消
应用

图 8

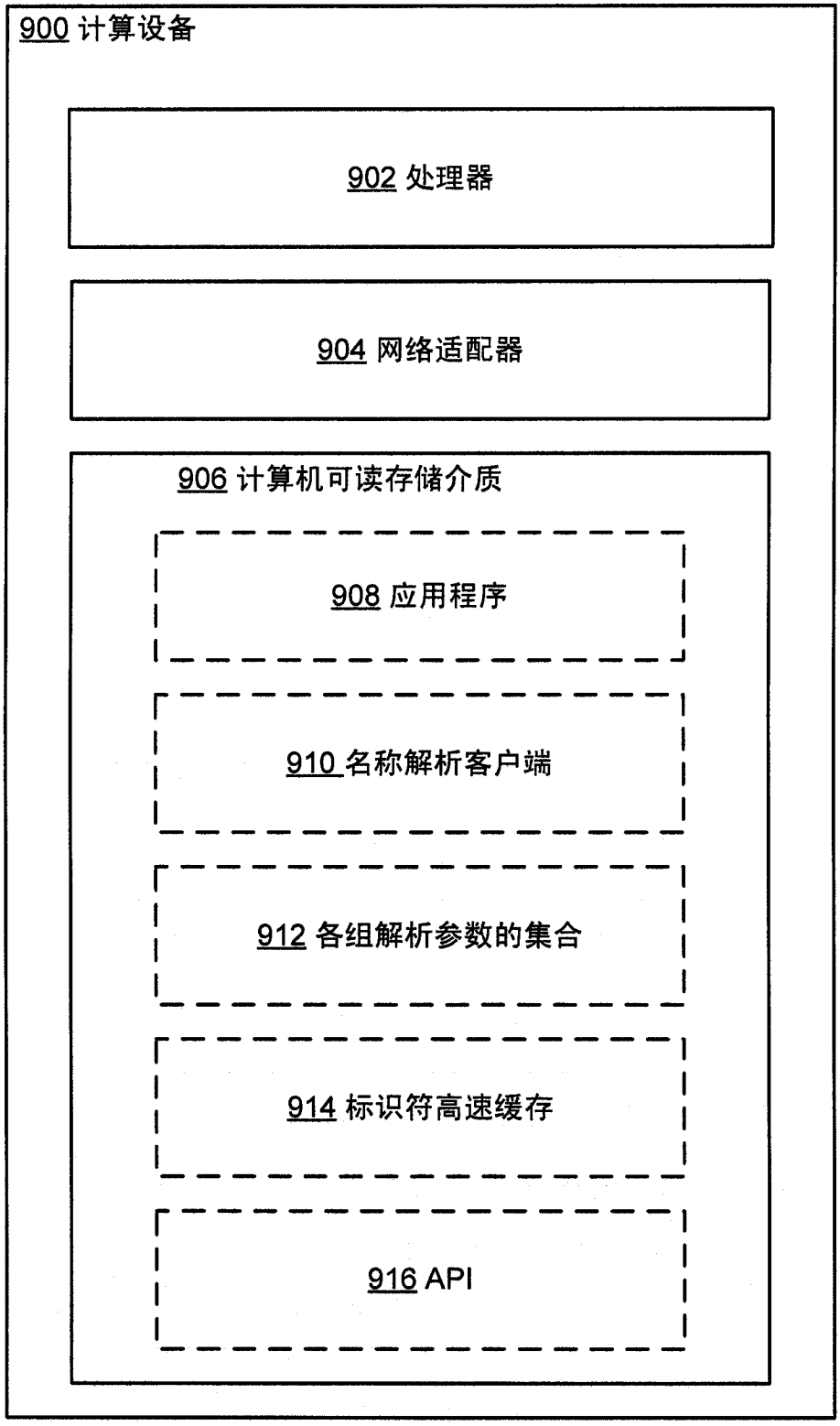

900 计算设备
902 处理器
904 网络适配器
906 计算机可读存储介质
908 应用程序
910 名称解析客户端
912 各组解析参数的集合
914 标识符高速缓存
916 API

图 9

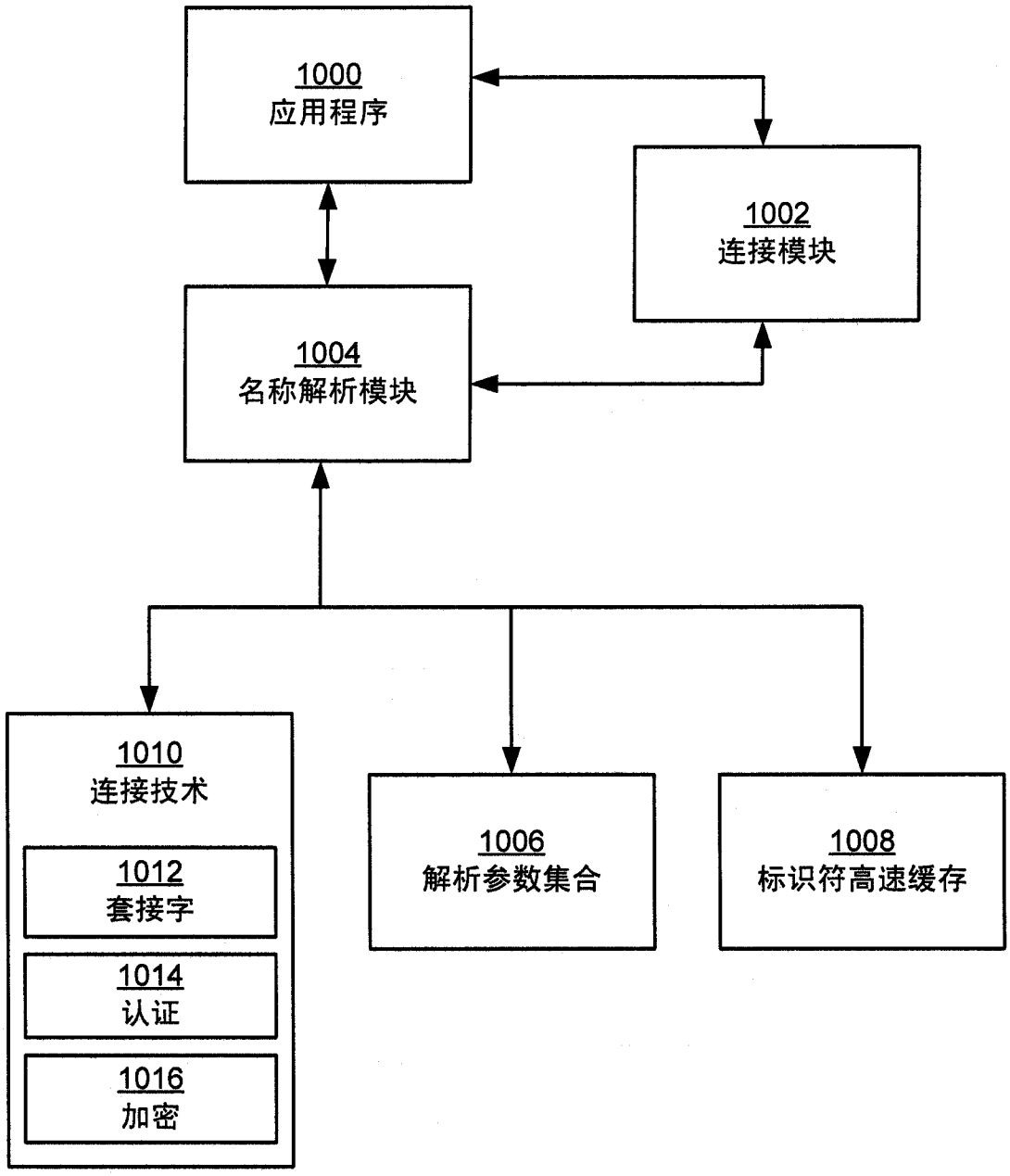

1000
应用程序
1002
连接模块
1004
名称解析模块
1010
连接技术
1012
套接字
1014
认证
1016
加密
1006
解析参数集合
1008
标识符高速缓存

图 10