(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111448557 B
(45)授权公告日 2024.07.30

(21)申请号 201880063309.1
(22)申请日 2018.07.30
(65)同一申请的已公布的文献号
申请公布号 CN 111448557 A
(43)申请公布日 2020.07.24
(30)优先权数据
62/539,504 2017.07.31 US
(85)PCT国际申请进入国家阶段日
2020.03.27
(86)PCT国际申请的申请数据
PCT/US2018/044444 2018.07.30
(87)PCT国际申请的公布数据
WO2019/027934 EN 2019.02.07

(73)专利权人 危机制止公司
地址 美国加利福尼亚州
(72)发明人 N·德海因 P·莫卡佩里丝 D·科波克 A·阿提沃 A·丘伊 T·L·伯恩斯
(74)专利代理机构 北京林达刘知识产权代理事务所(普通合伙) 11277
专利代理师 刘新宇

(51)Int.Cl.
G06F 15/173(2006.01)
(56)对比文件
US 2016380961 A1,2016.12.29
审查员 杨龙

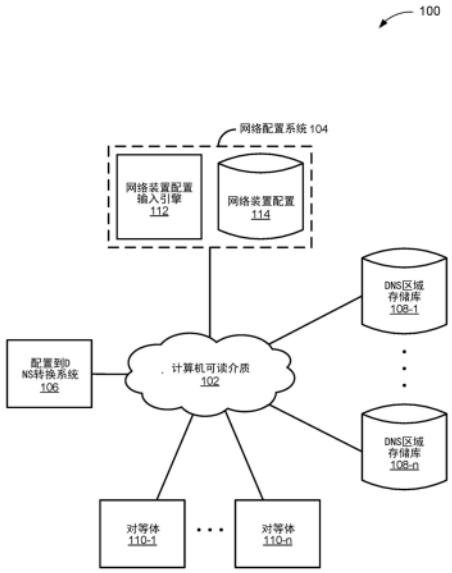
权利要求书2页 说明书13页 附图10页

(54)发明名称

利用网络节点传播信息

(57)摘要

公开了一种用于使用域名系统(DNS)来分配和获取与网络装置有关的信息的技术。使用DNS协议在一个或多个DNS服务和网络节点之间双向交换诸如配置设置和系统状况等的装置信息。交换的信息被编码为DNS记录。



CN 111448557 B

1.一种用于传播信息的方法,包括:

登录到网络装置传播服务门户;

进入网络装置配置设置;

获得网络装置配置传播代理和密钥,其中所述密钥是根据域名服务区域名称即DNS区域名称推导出的,所述DNS区域名称是根据客户的因特网协议地址即IP地址推导出的;

响应于来自对等体的触发刺激,将所述网络装置配置传播代理安装在所述对等体上;以及

将所述密钥安装在所述网络装置配置传播代理中,其中所述密钥提供所述DNS区域名称和与所述网络装置配置传播代理的安全通信。

2.根据权利要求1所述的方法,还包括:

下载具有网络装置配置数据的DNS记录;

存储网络装置配置;

检查网络装置配置更改。

3.根据权利要求2所述的方法,还包括在检测到网络装置配置更改的情况下:

下载具有网络装置配置数据的DNS记录;

存储所述网络装置配置数据;

检查网络装置配置更改。

4.根据权利要求2所述的方法,还包括:在尚未检测到网络装置配置更改的情况下,继续检查网络装置配置更改。

5.根据权利要求1、2、3和4中任一项所述的方法,还包括:

在多个预定的周期性间隔处收集遥测数据;

生成具有所述遥测数据的DNS记录;

进行动态DNS更新以将所述遥测数据中的至少一些遥测数据推送到网络装置配置传播服务。

6.一种用于传播信息的系统,包括:

用于登录到网络装置传播服务门户的部件;

用于进入网络装置配置设置的部件;

用于获得网络装置配置传播代理和密钥的部件,其中所述密钥是根据域名服务区域名称即DNS区域名称推导出的,所述DNS区域名称是根据客户的因特网协议地址即IP地址推导出的;

用于响应于来自对等体的触发刺激将所述网络装置配置传播代理安装在所述对等体上的部件;以及

用于将所述密钥安装在所述网络装置配置传播代理中的部件,其中所述密钥提供所述DNS区域名称和与所述网络装置配置传播代理的安全通信。

7.根据权利要求6所述的系统,还包括:

用于下载具有网络装置配置数据的DNS记录的部件;

用于存储网络装置配置的部件;

用于检查网络装置配置更改的部件。

8.根据权利要求7所述的系统,还包括:

用于在检测到网络装置配置更改的情况下下载具有网络装置配置数据的DNS记录的部件；

用于在检测到网络装置配置更改的情况下存储所述网络装置配置数据的部件；

用于在检测到网络装置配置更改的情况下检查网络装置配置更改的部件。

9.根据权利要求7所述的系统，还包括在尚未检测到网络装置配置更改的情况下继续检查网络装置配置更改的部件。

10.根据权利要求6、7、8和9中任一项所述的系统，还包括：

用于在多个预定的周期性间隔处收集遥测数据的部件；

用于生成具有所述遥测数据的DNS记录的部件；

用于进行动态DNS更新以将所述遥测数据中的至少一些遥测数据推送到网络装置配置传播服务的部件。

11.一种计算机程序产品，其包括如下指令，该指令在被计算机执行时使所述计算机执行根据权利要求1至5中任一项所述的方法的步骤。

利用网络节点传播信息

发明内容

[0001] 域名服务(DNS)协议用于向能够进行域名区域传送请求的网络装置、或者从能够进行动态DNS更新请求的网络装置传播信息。结合本文中所描述的技术的方法可以包括将配置信息从配置数据存储发送至网络装置。结合本文中所描述的技术的系统可以结合与将配置信息从配置数据存储发送至网络装置相关联的技术。结合本文中所描述的技术的方法可以包括将与网络装置的使用相关的信息发送至报告系统。结合本文中所描述的技术的系统可以结合与将与网络装置的使用相关的信息发送至报告系统相关联的技术。

附图说明

[0002] 图1描绘了对等触发网络装置配置传播系统的示例的图。

[0003] 图2描绘了从网络配置系统到DNS区域的对等触发网络装置配置传播所用的方法的示例的流程图。

[0004] 图3描绘了DNS服务器到DNS客户端网络装置配置传播系统的示例的图。

[0005] 图4描绘了DNS服务器到从或辅DNS服务器网络装置配置传播系统的示例的图。

[0006] 图5描绘了DNS引擎到DNS服务器网络装置遥测提供系统的示例的图。

[0007] 图6描绘了利用网络装置配置传播系统的方法的示例的流程图。

[0008] 图7描绘了具有多个传播控制器的网络装置配置传播系统的示例的图。

[0009] 图8描绘了具有防火墙的客户所使用的策略传播系统的示例的图。

[0010] 图9描绘了可以发生如本文中所描述的传播的结构的示例的图。

具体实施方式

[0011] 图1描绘了对等触发网络装置配置传播系统的示例的图100。图100包括计算机可读介质(CRM)102、网络配置系统104、配置到DNS转换系统106、DNS区域存储库108-1至DNS区域存储库108-n(统称为DNS区域存储库108)、以及对等体110-1至对等体110-n(统称为对等体110)。网络配置系统104、配置到DNS转换系统106、DNS区域存储库108和对等体110连接至CRM 102。

[0012] 本文中所论述的CRM 102和其它CRM意在包括法定的所有介质(例如,在美国,根据美国法典第35条第101款的所有介质),并且就针对包括有效的CRM的权利要求需要进行排除而言特别地排除本质上非法定的所有介质。已知的法定CRM包括硬件(例如,寄存器、随机存取存储器(RAM)、非易失性(NV)存储器等),但可以限于或者可以不限于硬件。

[0013] 本文中所讨论的CRM 102和其它计算机可读介质意在表示多种可能适用的技术。例如,CRM 102可以用于形成网络或网络的一部分。在两个组件共同位于装置上的情况下,CRM 102可以包括总线或者其它数据管道或数据面。根据特定实现或其它的考虑,CRM 102可以包括有线通信接口和无线通信接口,以通过有线或无线通信信道进行通信。在第一组件位于第一装置上、并且第二组件位于(不同的)第二装置上的情况下,CRM 102可以包括无线或有线的后端网络或LAN。CRM 102还可以包含WAN或其它网络的相关部分(如果适用的

话)。企业网络可以包括跨WAN段连接的地理分布式LAN。例如,分布式企业网络可以包括由WAN段分隔的多个LAN(在IEEE 802.11用语中,各LAN有时称为基本服务集(BSS),但是这里没有提出明确要求)。企业网络也可以使用VLAN隧道(在IEEE 802.11用语中,连接的LAN有时被称为扩展服务集(ESS),但是这里没有提出明确要求)。根据实现或其它考虑,CRM 102可以包括在企业或第三方的控制下的私有云、或公共云。

[0014] 本文中所描述的装置、系统和CRM可以被实现为计算机系统、计算机系统的部分或多个计算机系统。一般来说,计算机系统将包括处理器、存储器、非易失性存储器和接口。典型的计算机系统通常将至少包括处理器、存储器、以及将存储器连接至处理器的装置(例如,总线)。处理器可以例如是诸如微处理器等的通用中央处理单元(CPU)、或者诸如微控制器等的专用处理器。

[0015] 通过示例而非限制的方式,存储器可以包括诸如动态RAM(DRAM)和静态RAM(SRAM)等的随机存取存储器(RAM)。存储器可以是本地的、远程的或分布式的。总线还可以将处理器连接至非易失性存储器。非易失性存储器通常是磁性软盘或硬盘、磁光盘、光盘、(诸如CD-ROM、EPROM或EEPROM等的)只读存储器(ROM)、磁卡或光卡、或者用于大量数据的其它形式的存储器。在计算机系统上执行软件期间,通常通过直接存储器访问处理将该数据中的一些数据写入存储器。非易失性存储器可以是本地的、远程的或分布式的。非易失性存储器是可选的,这是因为可以利用存储器中可用的所有适用数据来创建系统。

[0016] 软件通常存储在非易失性存储器中。实际上,对于大型程序,甚至不可能将整个程序存储在存储器中。然而,应当理解,对于要运行的软件(如果必要的话),将该软件移动至适于处理的计算机可读位置,并且为了例示性目的,在本文中将该位置称为存储器。即使在将软件移动至存储器以供执行的情况下,处理器通常也会使用用以存储与软件相关联的值的硬件寄存器、以及理想地用于加速执行的本地高速缓存。如这里所使用的,在软件程序被称为“在计算机可读存储介质中实现”的情况下,假定该软件程序被存储在适用的已知或方便位置处(从非易失性存储器至硬件寄存器)。在与程序相关联的至少一个值被存储在处理器可读的寄存器中的情况下,认为该处理器“被配置为执行该程序”。

[0017] 在操作的一个示例中,可以通过作为包括文件管理系统(诸如盘操作系统等)的软件程序的操作系统软件来控制计算机系统。具有相关文件管理系统软件的操作系统软件的一个示例是已知为来自华盛顿州雷德蒙市微软公司的Windows®的一系列操作系统及其相关文件管理系统。操作系统软件及其相关文件管理系统软件的另一示例是Linux操作系统及其相关文件管理系统。文件管理系统通常存储在非易失性存储器中并且使处理器执行操作系统所需的各种动作以输入和输出数据以及将数据存储在存储器中,包括将文件存储在非易失性存储器上。

[0018] 总线还可以将处理器连接至接口。接口可以包括一个或多个输入和/或输出(I/O)装置。根据实现特定或其它的考虑,通过示例而非限制的方式,I/O装置可以包括键盘、鼠标或其它指示装置、盘驱动器、打印机、扫描仪以及包括显示装置的其它I/O装置。通过示例而非限制的方式,显示装置可以包括阴极射线管(CRT)、液晶显示器(LCD)、或者一些其它适用的已知或方便的显示装置。接口可以包括一个或多个调制解调器或网络接口。应当理解,调制解调器或网络接口可被认为是计算机系统的一部分。接口可以包括模拟调制解调器、ISDN调制解调器、线缆调制解调器、令牌环接口、卫星传输接口(例如“直接PC”)、或者用于

将计算机系统连接至其它计算机系统的其它接口。接口使计算机系统和其它装置能够在网络中连接在一起。

[0019] 计算机系统可以与基于云的计算系统兼容,或者作为基于云的计算系统的一部分或通过基于云的计算系统实现。如本文中所使用的,基于云的计算系统是向终端用户装置提供虚拟化的计算资源、软件和/或信息的系统。可以通过保持边缘装置可经由诸如网络等的通信接口访问的集中式服务和资源来使计算资源、软件和/或信息虚拟化。“云”可能是市场术语,并且为了本文的目的而可以包括这里所描述的任何网络。基于云的计算系统可以涉及服务的订阅或者使用公用定价模型。用户可以通过位于其终端用户装置上的web浏览器或其它容器应用来访问基于云的计算系统的协议。

[0020] 计算机系统可以作为引擎、引擎的一部分或者通过多个引擎而实现。如本文中所使用的,引擎包括一个或多个处理器或者一个或多个处理器的一部分。一个或多个处理器的一部分可以包括比组成任何给定的一个或多个处理器的全部硬件少的某一部分硬件,诸如寄存器的子集、多线程处理器的专用于一个或多个线程的处理器的一部分、或者处理器完全或部分地专用于执行引擎功能的一部分的时间片段等。正因如此,第一引擎和第二引擎可以具有一个或多个专用处理器,或者第一引擎和第二引擎可以与另一引擎或其它引擎共享一个或多个处理器。根据实现特定或其它的考虑,引擎可以是集中式的,或者其功能可以是分布式的。引擎可以包括硬件、固件或者包含在CRM中以供处理器执行的软件。诸如在本文中参考附图所描述的,处理器使用所实现的数据结构和方法来将数据转换为新数据。

[0021] 本文中所描述的引擎或者可以实现本文中所描述的系统和装置的引擎可以是基于云的引擎。如本文中所使用的,基于云的引擎是可以使用基于云的计算系统来运行应用和/或功能的引擎。全部或部分的应用和/或功能可以跨多个计算装置分布,并且无需限于仅一个计算装置。在一些实施例中,基于云的引擎可以执行终端用户通过web浏览器或容器应用所访问的功能和/或模块,而无需将该功能和/或模块本地安装在该终端用户的计算装置上。

[0022] 如本文中所使用的,数据存储意在包括具有任何适用的数据组织(包括表、逗号分隔值(CSV)文件、传统数据库(例如,SQL)、或其它适用的已知或方便的组织格式)的存储库。例如,数据存储可以被实现为嵌入在专用机器上的物理CRM中、嵌入在固件、硬件、它们的组合、或者适用的已知或方便的装置或系统中的软件。尽管数据存储相关组件(诸如数据库接口等)的物理位置和其它特性对于理解本文中所描述的技术而言并不重要,但数据存储相关组件可被认为是数据存储的“一部分”、某个其它系统组件的一部分、或它们的组合。

[0023] 数据存储可以包括数据结构。如本文中所使用的,数据结构与在计算机中存储和组织数据的具体方式相关联,使得可以在给定上下文内高效地使用该数据结构。数据结构一般基于计算机在其存储器内的任何位置(由地址、即本身可以存储在存储器中并且由程序操纵的位串指定)提取和存储数据的能力。因此,一些数据结构基于利用算术运算来计算数据项的地址;而其它数据结构基于利用结构本身来存储数据项的地址。许多数据结构使用这两个原则,有时以并非无意义的方式组合。数据结构的实现通常需要编写用于创建和操纵该结构的实例的过程的集合。本文中所描述的数据存储可以是基于云的数据存储。基于云的数据存储是与基于云的计算系统和引擎兼容的数据存储。

[0024] 返回到图1的示例,网络配置系统104意在表示企业网络的一部分,其可以包括负

责设置和维护网络装置配置的系统管理员和其它人员。在图100中,网络配置系统104包括网络装置配置输入引擎112和网络装置配置数据存储114。

[0025] 网络装置配置输入引擎112意在表示手动地、使用自动处理、或者通过这两种方式输入网络装置配置信息所经由的接口,诸如用于人输入数据的GUI等。例如,策略感知网络装置配置节点306或其代理中的一个或多个可以输入网络装置配置数据,网络装置配置输入引擎112将该网络装置配置数据存储在网络装置配置数据存储114中。

[0026] 在图1的示例中,配置到DNS转换系统106意在表示将来自网络配置系统104的网络装置配置转变为包括网络装置配置数据的DNS记录的系统。在特定实现中,对网络装置配置数据存储114的更改触发配置到DNS转换系统106以创建诸如DNS TXT记录等的DNS记录,其中该DNS记录对网络装置配置数据进行编码以供存储在DNS区域中。如本文所使用的,已被委托管理的一个或多个子域的区域称为DNS区域。

[0027] 对于上下文,顶级域名登记运营商可以向公众或具有法定地理或其它范围目的的实体提供名称空间,以登记二级域。负责较低级域的组织可以类似地操作其名称空间并对其空间进行细分。子域空间的每次登记或分配要求登记者维护行政和技术基础设施,以管理对于该区域的责任(包括转委托给较低级域)。区域从域边界开始直至包括域中的叶子节点(主机),或者在另一个独立管理的区域的边界结束。随着各域进一步划分为子域,各域本身变为具有其自己的管理员和DNS服务器的集合的DNS区域,树以底部的最大数量的叶子节点生长。在该最低级,在树的端节点或叶子中,术语“DNS区域”在使用和管理方面基本上与术语“域”同义。术语“域”在指派给它的实体的业务功能中使用,并且术语“区域”通常用于DNS服务的配置。

[0028] 在特定实现中,配置到DNS转换系统106使用DNS区域的知识(例如,已将管理责任委托给相应的单个管理员的DNS中的域名空间的不同、连续部分),以将与相应的多个DNS区域相关联并且可被识别为与相应的多个DNS区域相关联的DNS记录存储在DNS区域存储库108中。例如,配置到DNS转换系统106可以使与已更改的DNS区域相关联的授权开始(SOA)记录的序列号增加,其中该序列号将DNS区域标记为准备好进行传播。

[0029] 对于上下文,可以在操作系统文件中定义DNS区域,其中该操作系统文件以SOA开始,并且包含在该区域内描述的资源的记录。格式最初由伯克利因特网名称域服务器(BIND)软件包使用,并在通过引用而并入于此的RFC 1034和RFC 1035中定义。

[0030] 有利地,配置到DNS转换系统106使DNS记录包括网络装置配置,这使得网络装置配置能够如本文中稍后所述经由DNS服务进行分配。在可选方案中,作为替代或另外,DNS记录包括遥测数据。在又一可选方案中,作为替代或另外,DNS记录包括密钥管理数据。

[0031] 在图1的示例中,DNS区域存储库108意在表示在域名服务器的配置系统中所实现的DNS区域内描述的资源的记录。将网络装置配置消息存储在DNS区域存储库108中可被表征为将网络装置配置数据加载到DNS服务中以传播到适用的网络节点。DNS记录的示例是:

[0032] <device_id>.version1.config.threatstop.com 900IN TXT“param=value”

[0033] 在图1的示例中,对等体110意在表示具有有线或无线接口的装置,其中通过该有线或无线接口,对等体110可以在CRM 102上发送和接收数据。对等体110的示例是台式计算机、膝上型计算机、平板计算机、无线装置(诸如蜂窝电话或智能电话等)、或可穿戴式装置等。

[0034] 在特定实现中,对等体110包括可以在通过网络发送数据中使用的唯一标识符。唯一标识符可以包括根据因特网协议版本4(以下称为“IPv4”)创建的标识符、或根据因特网协议版本6(以下称为“IPv6”)创建的标识符,这两个协议版本均通过引用而并入于此。根据实现特定或其它的考虑,对等体110可以包括用于根据适用的无线装置协议接收和发送数据的适用通信接口。适用的无线装置协议的示例包括Wi-Fi、ZigBee®、蓝牙®和其它适用的低功耗通信标准。

[0035] 在特定实现中,对等体110用作站。本文中所使用的站可被称为具有到符合IEEE 802.11标准的无线介质的介质访问控制(MAC)地址和物理层(PHY)接口的装置。因此,例如,如果适用的话,网络装置可被称为站。IEEE 802.11a-1999、IEEE 802.11b-1999、IEEE 802.11g-2003、IEEE 802.11-2007和IEEE 802.11n TGn Draft 8.0(2009)通过引用而并入。如本文中所使用的,与802.11标准兼容或符合802.11标准的系统符合并入文献的要求和/或建议、或来自文献的早期草稿的要求和/或建议中的一个或多个的至少一些,并包括Wi-Fi系统。Wi-Fi是通常与IEEE 802.11标准、以及Wi-Fi保护访问(WPA)和WPA2安全标准以及可扩展认证协议(EAP)标准相关的非技术描述。在可选实施例中,站可以符合不同于Wi-Fi或IEEE 802.11的标准,可以被称为“站”之外的某个事物,并且可以具有到无线或其它介质的不同接口。

[0036] 在特定实现中,对等体110被配置为按照IEEE 802.3访问网络服务。IEEE802.3是工作组以及通过工作组定义有线以太网的物理层和数据链路层MAC而产生的IEEE标准的集合。这通常是利用一些广域网应用的局域网技术。通常由各种类型的铜缆或光缆在节点和/或基础设施装置(集线器、交换机、路由器)之间进行物理连接。IEEE 802.3是支持IEEE 802.1网络架构的技术。如相关领域中众所周知的,IEEE 802.11是工作组以及用于在2.4、3.6和5GHz频带中实现无线局域网(WLAN)计算机通信的标准的集合。标准IEEE 802.11-2007的基础版本随后进行了修订。这些标准为使用Wi-Fi品牌的无线网络产品提供了基础。IEEE 802.1和802.3通过引用而并入。

[0037] 在特定实现中,对等体110包括DNS引擎。根据实现或配置特定的因素,DNS引擎可以包括DNS服务器或DNS客户端。进一步根据实现或配置特定的因素,DNS引擎可以包括遥测子系统(未示出)或配置子系统,后者包括配置引擎和配置数据存储(未示出),稍后将讨论这两者。在一个或多个对等体110包括遥测子系统的实现中,网络配置系统104可以包括遥测读取器(未示出)。

[0038] 在操作示例中,诸如图1所示的系统如下操作。网络配置系统104通过CRM 102向配置到DNS转换系统106提供网络装置的配置设置。网络配置系统104可以响应于触发(诸如检测到网络装置配置的更改)而提供配置设置。网络装置配置设置可以包括网络装置的全部或部分配置。例如,网络装置配置设置可以仅包括增量,该增量是包括先前配置和当前配置之间的差异的部分配置。可以注意到,提供增量对于对等体施加了一些要求,这例如可以使用遥测子系统或配置子系统来管理。

[0039] 在该操作示例中,配置到DNS转换系统106将网络装置配置设置转换为DNS消息,该DNS消息存储在一个或多个DNS存储库108中。根据实现或配置特定的因素,网络装置配置设置可以以不适合封装(或包含)在适用的DNS消息中的格式提供,在这种情况下,配置到DNS转换系统106首先将网络装置配置设置转换为DNS消息兼容格式,然后将重新格式化的网络

装置配置设置包括在DNS消息中。在特定实现中,重新格式化的网络装置配置设置具有至少一个对等体110所理解的专有格式。在可选方案中,重新格式化的网络装置配置设置具有标准化格式。重新格式化可以包括或可以不包括加密,并且或者可以包括或可以不包括解密。

[0040] 在该操作示例中,DNS区域存储库108缓存要提供至对等体110的网络装置配置设置消息。在特定实现中,网络装置配置设置消息被提供至向网络配置系统104发起诸如AXFR查询或IXFR查询等的触发刺激的一个或多个对等体110。(RFC 5936、1995和1996通过引用而并入。)因此,网络装置配置设置消息是响应于来自对等体的触发刺激而提供的。另一方面,对于包括遥测读取器的网络配置系统104,可能不需要向对等体提供网络装置配置设置消息。相反,DNS区域存储库108可以根据遥测读取器、并且响应于动态DNS更新而更新。该可选方案可能需要在一个或多个对等体110处实现遥测引擎。

[0041] 负责提供网络装置配置的一方与将网络装置配置转换为DNS兼容格式的一方不需要是同一方。例如,DNS服务的客户可以向DNS服务提供网络装置配置,该DNS服务在客户发送DNS查询或动态DNS更新时将网络装置配置转换为DNS兼容格式。从概念上讲,网络配置系统104和配置到DNS转换系统106可以被表征为DNS服务的一部分。具体地,网络配置系统104将至少包括用于缓存数据以供配置到DNS转换系统106使用的数据存储,并且甚至是最简的缓冲器也可以被表征为在DNS服务的控制下的网络配置系统。类似地,DNS区域存储库108至少包括DNS服务从中传播DNS区域存储库108的DNS记录的缓冲器。另一方面,对等体110可能在DNS服务的一个或多个客户的控制下。

[0042] 在该操作示例中,对等体110或与其相关联的代理通过DNS查询触发网络配置系统104,并且对等体110接收包括更新后的网络装置配置的相应响应。例如,在网络配置系统104、配置到DNS转换系统106和DNS区域存储库108由DNS服务控制的情况下,DNS服务的客户可以经由对等体110其中之一或某个其它装置以及来自对等体110其中之一的触发,来提供网络装置配置。DNS服务可能还期望接收来自客户的遥测数据。因此,为了例示性目的,在该操作示例中,客户将遥测数据发送回DNS服务。

[0043] 如先前所示,遥测子系统可能不必要地对适用的对等体进行显式DNS响应,尽管对等体110仍然通过例如动态DNS更新来触发网络装置配置传播。在任何情况下,上述操作示例提供了对于从网络配置系统到DNS区域的对等触发网络装置配置传播的理解。

[0044] 图2描绘了从网络配置系统到DNS区域的对等触发网络装置配置传播所用的方法的示例的流程图200。该流程图以及本文中所描述的其它流程图示出以有助于理解的方式组织的模块(和潜在的决策点)。然而,应当认识到,在情况允许的情况下,可以对模块进行重组,以并行执行、重新排序、修改(更改、移除或增强)。流程图200从模块202开始:创建、读取、更新或删除(CRUD)网络装置配置。在特定实现中,系统操作员或自动处理配置网络装置。系统操作员或自动处理可能与DNS服务的客户相关联。可以注意到,读取、创建然后删除、以及更新和更新以撤消先前的更新可能导致没有净增量。然而,这种活动可能触发其它处理,诸如安全处理等。

[0045] 在图2的示例中,流程图200继续到模块204:响应于CRUD而触发网络装置配置传播处理。如何检测CRUD是实现和/或配置特定的。例如,检测CRUD指示、检测数据存储访问或者识别当前数据存储相对于先前数据存储的增量等可能会触发该处理。有利地,网络装置配置可以以与要使用DNS传播的一个或多个DNS区域相关联的DNS记录的形式缓冲。

[0046] 在图2的示例中,流程图200继续到模块206:将网络装置配置数据并入到DNS记录中。

[0047] 在图2的示例中,流程图200继续到模块208:向DNS服务提供DNS记录。有利地,尽管实际上该DNS记录包括网络装置配置数据,但是DNS服务可以将该DNS记录视为与任何其它DNS记录一样,。网络装置配置传播处理不是策略传送,因为策略是由例如系统操作员或自动处理预先设置的。这里将这种处理称为策略无关网络装置配置传播处理。

[0048] 在图2的示例中,流程图以模块210结束:在DNS区域内传播策略无关网络装置配置。在特定实现中,为区域设置策略的一方是向DNS服务提供网络装置配置、然后触发DNS服务以在DNS区域内传播网络装置配置的一方。由于DNS服务不传送策略,因此传播可以被表征为策略无关。有利地,网络装置可被配置为使用DNS服务所提供的DNS区域或使用不同的DNS区域。无论如何,多个网络装置可以以这种方式从同一DNS服务中检索配置。

[0049] 图3描绘了DNS服务器到DNS客户端网络装置配置传播系统的示例的图300。图300包括网络302、连接至网络302的策略无关网络装置配置传播节点304、以及连接至网络302的策略感知网络装置配置节点306-1至策略感知网络装置配置节点306-n(统称为策略感知网络装置配置节点306)。

[0050] 在图3的示例中,为了例示性目的,网络302意在包括LAN、WAN、某一其它大小的网络或其组合。在特定实现中,策略无关网络装置配置传播节点304和策略感知网络装置配置节点306经由因特网协议(IP)技术操作连接。例如,策略无关网络装置配置传播节点304和策略感知网络装置配置节点306可以跨私有网络或者跨公共网络(诸如因特网等)存在。

[0051] 在图3的示例中,策略无关网络装置配置传播节点304意在表示提供DNS服务的节点,其中通过该DNS服务,根据策略感知网络装置配置节点306的策略来提供网络装置配置。在图300中,策略无关网络装置配置传播节点304包括DNS区域存储库308-1至DNS区域存储库308-n(统称为DNS区域存储库308)以及DNS服务器310-1至DNS服务器310-n(统称为DNS服务器310)。

[0052] 在图3的示例中,DNS区域存储库308意在表示被配置为存储与一个或多个网络装置相关联并具有该一个或多个网络装置的网络装置配置信息的DNS记录的数据存储。

[0053] 在图3的示例中,DNS服务器310意在表示以具有网络装置配置数据的DNS记录对DNS查询进行响应的引擎,其中策略感知网络装置配置节点306使用该网络装置配置数据来配置网络装置。

[0054] 在图3的示例中,策略感知网络装置配置节点306意在表示向策略无关网络装置配置传播节点304发送DNS查询以触发包括网络装置配置数据的DNS响应的节点,其中策略感知网络装置配置节点306使用该网络装置配置数据来配置网络装置。在图300中,策略感知网络装置配置节点306包括网络装置配置传播触发引擎312、DNS客户端314、DNS区域内容到配置数据转换引擎316、配置引擎318、以及网络装置配置数据存储320。

[0055] 在特定实现中,网络装置配置传播触发引擎312向DNS客户端314发出DNS请求。根据实现或配置特定的因素,一个或多个DNS服务器310可以在区域数据发生更改时向DNS客户端314发送NOTIFY(通知)消息,尽管区域传送的调度完全由网络装置配置传播触发引擎312控制。在特定实现中,网络装置配置传播触发引擎312以规则的间隔、以由区域顶点的SOA资源记录中的“刷新”、“重试”和“期满”字段的值控制的模式调度区域传送。触发的频率

和周期取决于实现或配置特定的因素,诸如触发是手动的还是自动的。

[0056] 在特定实现中,DNS客户端314首先连接至DNS服务器310其中之一。诸如传送层安全(TLS)或其前身安全套接字层(SSL)等的加密协议可以在网络302上提供通信安全。有利地,由于用于对所发送的数据进行加密的对称加密,可以使连接安全。这种对称加密所用的密钥是针对各连接唯一生成的,并且是基于会话开始时协商的共享机密。DNS服务器310和DNS客户端314在发送数据之前协商要使用哪些加密算法和加密密钥的详情。可选地或另外,DNS服务器310和DNS客户端314的身份可以使用一方或双方可能需要的公共密钥加密进行认证。可选地或另外,各消息包括使用消息认证码的消息完整性检查,以防止未检测到发送期间的数据丢失或变更。以这种方式,连接可以确保完整性。

[0057] 在DNS客户端314连接至DNS服务器310其中之一后,DNS客户端314发起DNS异步完全区域传送(AXFR)。区域传送使用传输控制协议(TCP)进行传输。DNS服务器310和DNS客户端314这样命名是因为区域传送采用客户端-服务器事务的形式。应当注意,请求区域传送的客户端可以是从主服务器请求数据的从服务器或辅服务器。

[0058] 区域传送包括前导码,然后是实际数据传送。前导码包括“区域顶点”的授权开始(SOA)资源记录的查找,其中“区域顶点”是位于“区域”顶部的DNS名称空间的节点。该SOA资源记录的字段、特别是“序列号”判断是否需要进行实际数据传送。客户端将SOA资源记录的序列号与其具有的该资源记录的最后副本中的序列号进行比较。如果正在传送的记录的序列号增大,则区域中的数据被视为“已更改”(以某种方式),并且从属方继续请求实际区域数据传送。如果序列号相同,则区域中的数据将不被视为“已更改”,并且客户端可以继续使用它已经拥有的数据库的副本(如果客户端具有该副本的话)。

[0059] 在特定实现中,DNS客户端314使用DNS查询解决机制来进行前导码的SOA查找。在DNS客户端314识别出需要进行实际数据传送之前,DNS客户端314不会打开到DNS服务器310其中之一的TCP连接。在可选方案中,DNS客户端314在进行前导码的SOA查找之前打开到DNS服务器310其中之一的TCP连接,因为它们继而(可以)通过同一TCP连接进行实际数据传送。

[0060] 实际数据传送处理以DNS客户端314通过到DNS服务器310其中之一的TCP连接发送具有特定查询类型AXFR(值252)的查询(操作码0)开始。DNS服务器310以一系列响应消息进行响应,其中该一系列响应消息包括区域中的每个域名的所有资源记录。第一个响应包括区域顶点的SOA资源记录。其它数据不遵循指定顺序。数据的末端由重复包含区域顶点的SOA资源记录的响应的相关DNS服务器310以信号形式通知。

[0061] DNS客户端314可以使用事务签名(TSIG)来对包含DNS客户端314的策略感知网络装置配置节点306其中之一进行认证。TSIG使用共享机密密钥和单向散列来提供将DNS服务器310和DNS客户端314认证为允许进行DNS更新或对DNS更新进行响应的加密安全方式。根据实现或配置特定的因素,对DNS的查询可以在不认证的情况下进行,但对DNS的更新必须进行认证。在TSIG协议中包括时间戳,以防止重复使用所记录的响应。这可能要求DNS服务器310和DNS客户端314具有准确的时钟。网络时间协议可以提供准确的时间源。与查询一样,DNS更新通常经由UDP来传输,但是DNS服务器310可以支持UDP和TCP请求这两者。TSIG在通过引用而并入的RFC 2845中进行了描述。

[0062] 除非另有中断,否则DNS客户端314最终使来自AXFR响应的网络装置配置数据可用于DNS区域内容到配置数据转换引擎316。

[0063] DNS区域内容到配置数据转换引擎316读取响应或至少读取区域内容,并从响应中解码网络配置数据。如果信息包括校验和,则DNS区域内容到配置数据转换引擎316可以利用校验和处理来确保其完整性。DNS区域内容到配置数据转换引擎316向配置引擎318提供网络装置配置数据。

[0064] 配置引擎318将配置写入网络装置配置数据存储320。配置数据存储320的典型实现是作为“配置文件”;配置文件的强大传统在于人可编辑的纯文本,并且简单的密钥-值对格式是常见的。有利地,本文中所描述的技术便于在DNS记录中编码数据时使用文本、并以安全的方式传递这种易于使用的格式。在可选方案中,使用状态信息来触发其它软件处理。

[0065] 在操作示例中,诸如图3所示的系统如下操作。响应于对一个或多个DNS区域存储库308的更改,一个或多个DNS服务器310可以将NOTIFY消息从策略无关网络装置配置传播节点304发送到一个或多个策略感知网络装置配置节点306。在可选方案中,DNS服务器310不发送NOTIFY消息。

[0066] 在该操作示例中,网络装置配置传播触发引擎312判断是否要发起网络装置配置传播处理。在DNS服务器310能够发送NOTIFY消息的情况下,网络装置配置传播触发引擎312可以响应于接收到NOTIFY消息而发起处理。可选地,在DNS服务器310不发送NOTIFY消息的情况下,或者除了对NOTIFY消息响应而进行动作之外,网络装置配置传播触发引擎312可以周期性地发起处理或者响应于(例如,系统管理员的)明确指示而发起处理。网络装置配置传播触发引擎312在确定(正确或不正确)相关的一个或多个DNS区域存储库308未被更改的情况下可以选择不采取周期性动作。为了触发处理,网络装置配置传播触发引擎312向DNS客户端314发送DNS请求。

[0067] 在该操作示例中,DNS客户端314通过网络302与相关的一个DNS服务器310建立连接。假设连接不由于例如判断为自上次区域传送以来尚未对相关的一个或多个DNS区域存储库308进行更改而被中止,则DNS客户端314向DNS服务器310发送DNS区域传送(例如,AXFR)查询,该DNS服务器310以包括网络装置配置数据的DNS响应进行响应。

[0068] 在该操作示例中,DNS区域内容到配置数据转换引擎316将网络装置配置数据内容解码为适合由配置引擎318存储在网络装置配置数据存储320中的格式。

[0069] 图4描绘了DNS服务器到从或辅DNS服务器网络装置配置传播系统的示例的图400。图400包括网络402、连接至网络402的策略无关网络装置配置传播节点404、以及连接至网络402的策略感知网络装置配置节点406-1至策略感知网络装置配置节点406-n(统称为策略感知网络装置配置节点406)。图400与图300类似,但是DNS客户端314被DNS服务器414取代。在图4的示例中,DNS服务器410与DNS服务器310(图3)类似,并且DNS区域存储库408是可选的。具体地,区域传送请求可以包括如参考图3通过示例的方式所述的AXFR查询、或者用于增量区域传送的IXFR查询。

[0070] 增量区域传送与完全区域传送在以下方面有所不同:第一,DNS服务器414(用作DNS客户端)使用QTYPE IXFR(值251)而不是AXFR QTYPE。第二,DNS服务器414在IXFR消息中发送其当前具有的区域顶点的SOA资源记录(如果有的话),让服务器知道“区域”的哪个版本被认为是当前的。第三,尽管相关的一个DNS服务器410可以采用正常AXFR方式以区域的完全数据进行响应,但作为替代,它也可以以“增量”数据传送进行响应。后者包括在客户端向服务器报告为具有的区域版本和服务器上当前的区域版本之间按区域序列号顺序对区

域数据的更改的列表。这些更改包括两个列表,一个是删除的资源记录,并且一个是插入的资源记录。(对资源记录的修改表示为删除然后插入。)

[0071] 除DNS服务器414外,策略感知网络装置配置节点406还包括网络装置配置传播触发引擎412、DNS区域内容到配置数据转换引擎416、配置引擎418和网络装置配置数据存储420。由于策略感知网络装置配置节点406具有服务器(DNS服务器414),因此在策略感知网络装置配置节点406的下游可以存在或可以不存在具有DNS引擎(服务器或客户端)的附加对等体。

[0072] 图5描绘了DNS引擎到DNS服务网络装置遥测提供系统的示例的图500。图500包括网络502、连接至网络502的网络装置配置客户节点504-1至网络装置配置客户节点504-n(统称为网络装置配置客户节点504)、以及网络装置配置服务节点506。

[0073] 在图5的示例中,为了例示性目的,网络502意在包括LAN、WAN、某一其它大小的网络或其组合。在特定实现中,网络装置配置客户节点504和网络装置配置服务节点506经由因特网协议(IP)技术操作连接。例如,网络装置配置客户节点504和网络装置配置服务节点506可以跨私有网络或公共网络(诸如因特网等)存在。

[0074] 在图5的示例中,网络装置配置客户节点504意在表示在经由DNS接收网络装置配置服务的实体的控制下的引擎和数据存储。在图500中,网络装置配置客户节点504包括遥测报告触发引擎508、网络装置配置到DNS区域内容转换引擎510、反馈到DNS区域内容转换引擎512、配置数据存储514、反馈数据存储516、以及DNS引擎518(其可以包括DNS服务器或DNS客户端)。

[0075] 遥测报告触发引擎508意在表示负责发起信息收集处理的引擎,该信息收集处理最终向网络装置配置服务节点506提供遥测。在特定实现中,遥测报告触发引擎508包括引起周期性触发刺激以发起遥测处理的定时器。作为替代或另外,遥测报告触发引擎508可以响应于发起遥测处理的明确命令(例如,由人或其代理提供的“手动”指示)而这样做。

[0076] 当发起该处理时,遥测报告触发引擎508使网络装置配置到DNS区域内容转换引擎510和反馈到DNS区域内容转换引擎512分别访问配置数据存储514和反馈数据存储516,并将网络装置配置数据和反馈转换为DNS记录,以供DNS引擎518发送至网络装置配置服务节点506。

[0077] 反馈数据存储516中的反馈可以包括软件命令所返回的信息、日志数据或网络的特性(诸如设置、软件版本信息、错误状况或性能数据等)。正如网络装置配置到DNS区域内容转换引擎510将网络装置配置数据编码为具有网络装置配置数据的诸如DNS文本记录(DNS TXT记录)等的DNS记录,反馈到DNS区域内容转换引擎512将反馈编码为具有反馈数据的DNS记录。

[0078] DNS引擎518能够进行DNS请求。如果使用公共DNS基础设施,则DNS引擎518被配置有相关DNS区域的名称。在操作中,DNS引擎518连接至网络装置配置服务节点506。在特定实现中,使用相互认证(诸如由TLS提供的认证等)。在特定实现中,DNS引擎518对其配置中所提供的DNS区域进行动态DNS更新。动态DNS更新可以用DNS TSIG密钥签名,从而对相关的一个网络装置配置客户节点504进行认证。如果使用私有DNS基础设施,则DNS配置可能需要包括适用DNS服务器的IP地址或主机名称。DNS记录的示例是:

[0079] <device_id>.version1.tele.threatstop.com 900IN TXT“telemetry=value”

[0080] 在图5的示例中,网络装置配置服务节点506意在表示在使用DNS提供网络装置配置传播服务的实体的控制下(或与客户的共享控制下)的引擎和数据存储。在图500中,网络装置配置服务节点506包括DNS服务器520-1至DNS服务器520-n(统称为DNS服务器520)、DNS区域存储库522-1至DNS区域存储库522-n(统称为DNS区域存储库522)、DNS区域内容到配置数据转换引擎524、配置引擎526和网络装置配置数据存储528。

[0081] 动态DNS更新由相关的一个DNS服务器520接收并处理,从而创建DNS记录以存储在相关的一个DNS区域存储库522中。DNS服务器520可以是公共或私有DNS基础设施的一部分。在特定实现中,DNS区域内容到配置数据转换引擎524响应于手动或自动触发,使用DNS区域传送(例如,AXFR)来读取DNS区域存储库522中所包含的DNS区域的内容,对DNS记录进行解码,并向配置引擎526提供网络装置配置数据,其中配置引擎526将配置数据存储在网络装置配置数据存储528中。有利地,多个网络装置配置客户节点504可以向网络装置配置服务节点506散布信息。各网络装置配置客户节点504可被配置为使用由网络装置配置服务节点506提供的相同DNS区域,或者一个或多个网络装置配置客户节点504可以使用不同的DNS区域。

[0082] 图6A、6B和6C描绘了利用网络装置配置传播系统的方法的示例的流程图600。流程图600从模块602(图6A)开始:登录到网络装置配置传播服务门户。在特定实现中,由登录期间可获得的IP地址推导出区域名称。根据实现或配置特定的因素,还可以在客户或其代理登录期间或之后显式提供区域名称。

[0083] 在图6A的示例中,流程图600继续到模块604:进入网络装置配置设置。有利地,在DNS记录中对网络装置配置设置进行编码,以利用DNS基础设施。根据实现或配置特定的因素,客户可以进入如DNS记录、或通过网络装置配置传播服务或其代理而转换为DNS记录的某些其它格式的网络配置设置。

[0084] 在图6A的示例中,流程图600继续到模块606:获得网络装置配置传播代理和密钥。在特定实现中,下载网络装置配置传播代理。在可选方案中,代理是流式传输的,在运行时虚拟提供的,或者以某些其它方式对客户可用的。在特定实现中,密钥由DNS区域名称(客户显式提供、由客户的IP地址推导出,或者以某些其它方式获得)推导出,或者由与相关区域相关联的密钥(诸如TSIG等)推导出。

[0085] 在图6A的示例中,流程图600继续到模块608:将网络装置配置传播代理安装在对等体上。根据实现或配置特定的因素,客户可以具有一个或多个对等体。在特定实现中,一个实体(网络装置配置传播服务)是所有对等体的服务提供商。在可选方案中,网络装置配置传播服务具有分布在整个对等网络中的功能。

[0086] 在图6A的示例中,流程图600继续到模块610:将密钥安装在网络装置配置传播代理中。密钥可用于提供从中推导出该密钥的DNS区域名称、以及与网络装置配置传播服务的安全通信。从模块610开始,流程图600划分为分别与传播和遥测相关联的两个不同路径。

[0087] 在图6B的示例中,流程图600继续到模块612:下载具有网络装置配置数据的DNS记录。在特定实现中,进行应用级安全校验(诸如校验和等)以验证网络装置配置数据。有利地,校验和使对等体能够知道配置是何时完成的(这是一个现实问题)。

[0088] 在图6B的示例中,流程图600继续到模块614:存储网络装置配置。在特定实现中,DNS记录在存储之前被解码。

[0089] 在图6B的示例中,流程图600继续到模块616:检查网络装置配置更改。在特定实现中,可以周期性地或利用明确指示手动地触发检查。

[0090] 在图6B的示例中,流程图600继续到决策点618,其中在该决策点618处判断是否检测到网络装置配置的更改。如果判断为已检测到网络配置设置的更改(618-“是”),则流程图600返回到模块612并从该模块继续。另一方面,如果判断为未检测到网络装置配置的更改(618-“否”),则流程图600重复模块616和决策点618,直到检测到网络装置配置的更改为止。

[0091] 在图6C的示例中,流程图600(从模块610开始)继续到模块620:收集遥测数据。在特定实现中,周期性地收集遥测数据。周期可能根据需要而变化,但在特定实现中,15分钟被认为是足够细粒度。

[0092] 在图6C的示例中,流程图600继续到模块622:生成具有遥测数据的DNS记录。

[0093] 在图6C的示例中,流程图600继续到模块624:进行动态DNS更新以将遥测数据推送到网络装置配置传播服务。在特定实现中,网络装置配置传播服务对DNS记录进行解码并存储在其中编码的遥测数据。然后,流程图600返回到模块620并如前所述继续,从而创建包括模块620、622和624的循环。

[0094] 图7描绘了具有多个传播控制器的网络装置配置传播系统的示例的图700。图700包括控制器702、控制器704、对等体706和对等体708。控制器702、704包括一个或多个DNS服务器以及DNS区域存储库。(未示出,但参见图1～6以获得对这些组件的讨论。)对等体706、708包括DNS引擎,诸如DNS服务器或DNS客户端等。(未示出,但参见图1～6以获得对这些组件的讨论。)对等体可以被配置在或可以不被配置在不相关的DNS域中。图700意在示出网络装置配置传播服务可以由多于一个控制器进行控制。

[0095] 在图7的示例中,控制器702、704意在表示适合将网络装置配置传播至多个对等体的DNS区域存储库和相关引擎。在图7的示例中,控制器702参与来自对等体706、708的写入访问以及通过对等体708的读取访问,而控制器704参与通过对等体706、708的读取访问。这些访问仅为了例示性目的;控制器704无需被表征为仅限于来自对等体的读取访问。然而,也可以限制允许的访问形式。例如,对等体706只能进行对控制器702的写入访问以及对控制器704的读取访问,而对等体708只能从控制器704进行读取,但可以从控制器702进行读取和写入。

[0096] 有利地,对等体706、708可以通过对控制器702、704的DNS服务的共享访问来交换响应策略记录(DNS RPZ记录),因此无需集中式系统来分配信息。

[0097] 图8描绘了具有防火墙的客户所使用的策略传播系统的示例的图800。图800包括主系统802和客户系统804。在图8的示例中,主系统802意在表示在该特定示例中传播策略的服务(或控制器)。

[0098] 在图800中,主系统802包括策略子系统806、策略到DNS转换引擎808和主DNS服务810。在图8的示例中,策略子系统806意在表示生成网络过滤策略(诸如可以由网络防火墙进行过滤的域名和IP网络的列表)的引擎和数据存储。策略到DNS转换引擎808将策略转换为诸如DNS RPZ记录、文本记录、编码字符串数据记录等的DNS记录,这些DNS记录不必限于DNS记录类型。DNS记录被加载到由主DNS服务810服务的DNS区域中。

[0099] 在图800中,客户系统804包括防火墙812-1至防火墙812-n(统称为防火墙812)以

及客户DNS服务814。防火墙812与各个网络节点相关联。在特定实现中,防火墙进行DNS请求。例如,防火墙812可以向主DNS服务810发出DNS区域传送请求,以检索包含网络过滤策略的一个或多个DNS区域并对通过防火墙812的网络业务应用网络策略。防火墙向客户DNS服务814发出动态DNS更新。例如,防火墙812可以发送表示域名或IP子网的DNS记录,以增强或修改网络过滤策略。其它防火墙812可以检索这些DNS记录,并将DNS记录应用到该其它防火墙812的策略。有利地,可以如参考图7所述利用多个对等体、以及如参考图1～6所述利用网络配置系统来跨多个控制器地应用参考图8所述的系统。

[0100] 应当注意,单个实体可以控制多个控制器。例如,条例可能要求为不同权限设置服务块。在该示例中,服务可以用多个控制器实现,其中各控制器与不同的权限相关联。不同的实体也可以控制多个不同的控制器。例如,第一实体可以使用第一控制器进行网络装置配置传播,第二实体可以使用第二控制器进行遥测,并且第三实体可以使用第三控制器用于广告网站策略。有利地,不同方可以仅共享所涉及的各实体可接受的事物来一起工作。例如,私有实体可能不想让其黑名单或白名单公布于众。

[0101] 图9描绘了可能发生如本文中所描述的传播的结构的示例的图900。图900包括根节点902、DNS服务器904-1至DNS服务器904-n(统称为DNS服务器904)、DNS服务器906、以及DNS客户端908-1至DNS客户端908-n(统称为DNS客户端908)。根节点902意在表示DNS区域的根节点数据。根节点数据可以跨许多服务器(未示出)进行复制。DNS服务器904是向其它DNS服务器或客户端提供根节点数据的服务器。从理论上讲,DNS服务器904和DNS服务器906(意在表示仅以DNS客户端908作为孩子的边缘服务器)之间可以存在任意数量的服务器。DNS服务器906可以通过存活时间日期代码缓存来实现。

[0102] 有利地,传播服务可以提供到ALT根(rootid)的路径,该路径是存活在主系统或控制器上的完全不同的树。尽管TSIG不是为了访问控制而设计的,但在特定实现中,主系统或控制器使用TSIG来进行访问控制和数据验证这两者(后者是设计TSIG的目的)。

[0103] 本文中所提供的这些和其它示例意在说明而不必限制所描述的实现。如这里所使用的,术语“实现”意味着用于通过示例而非限制的方式进行说明的实现。先前的文本和图中所描述的技术可以根据情况需要进行混合和匹配,以产生可选实现。

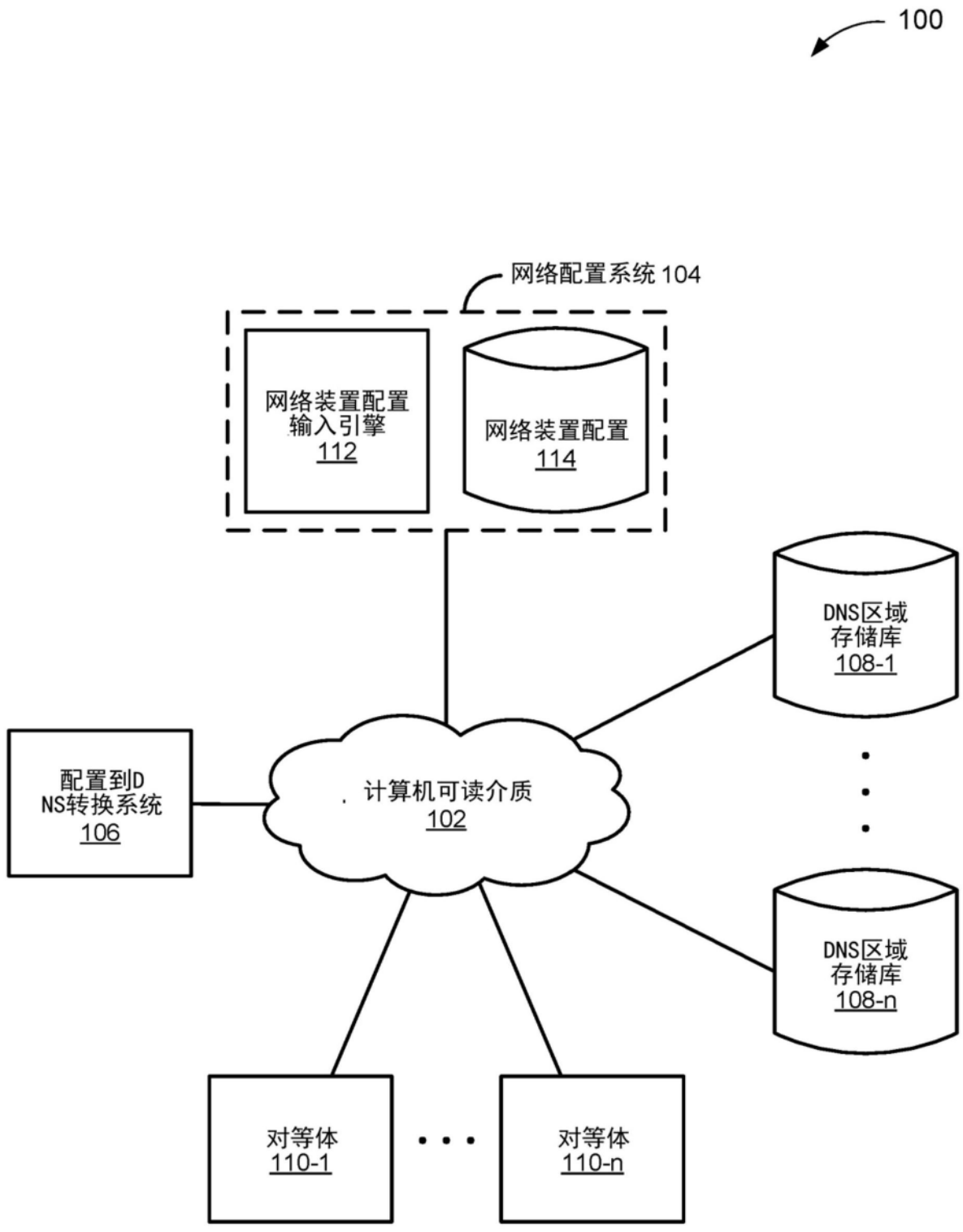

100
网络配置系统 104
网络装置配置
输入引擎
112
网络装置配置
114
DNS区域
存储库
108-1
配置到D
NS转换系统
106
计算机可读介质
102
DNS区域
存储库
108-n
对等体
110-1
对等体
110-n

图1

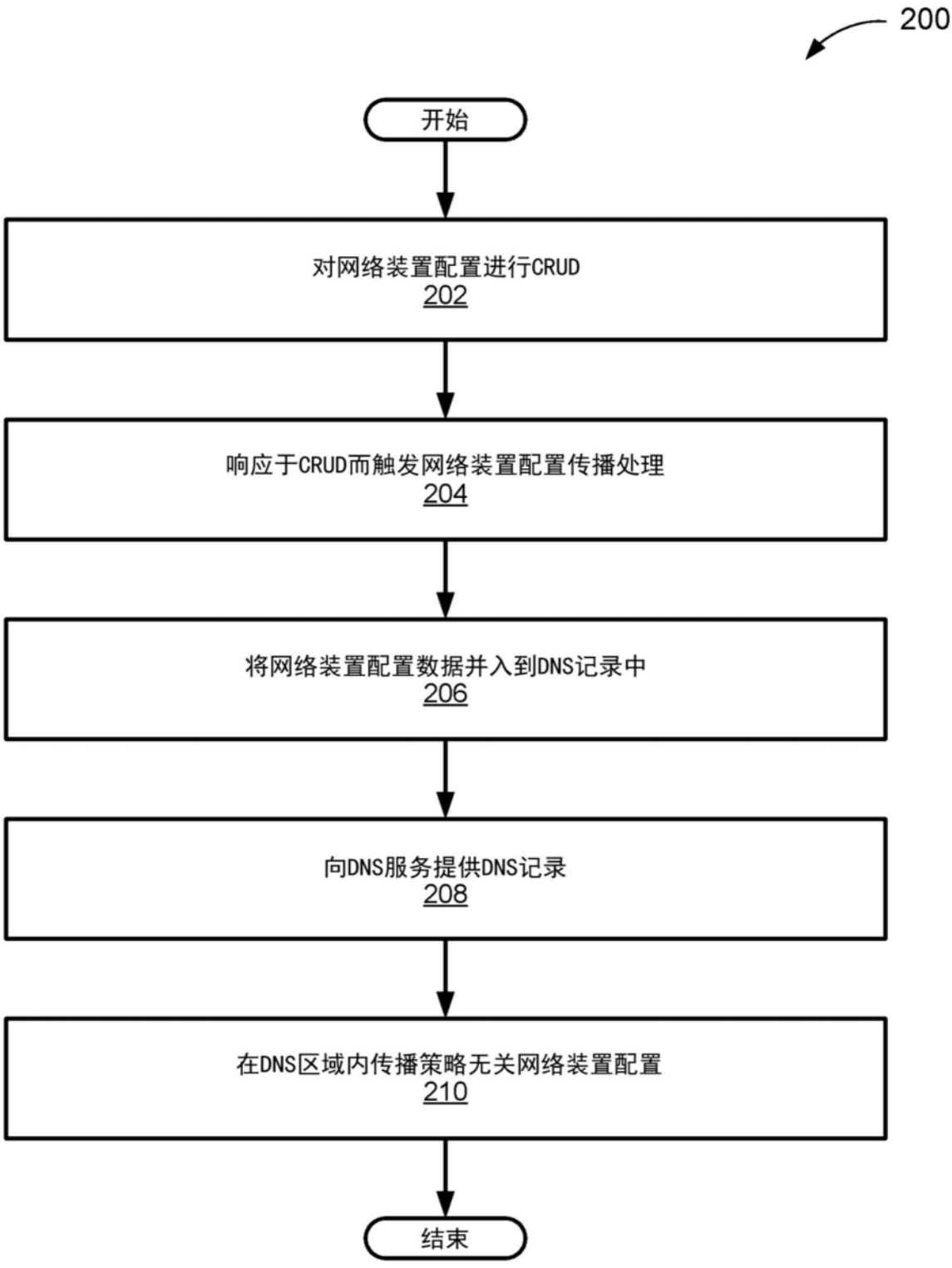

200
开始
对网络装置配置进行CRUD
202
响应于CRUD而触发网络装置配置传播处理
204
将网络装置配置数据并入到DNS记录中
206
向DNS服务提供DNS记录
208
在DNS区域内传播策略无关网络装置配置
210
结束

图2

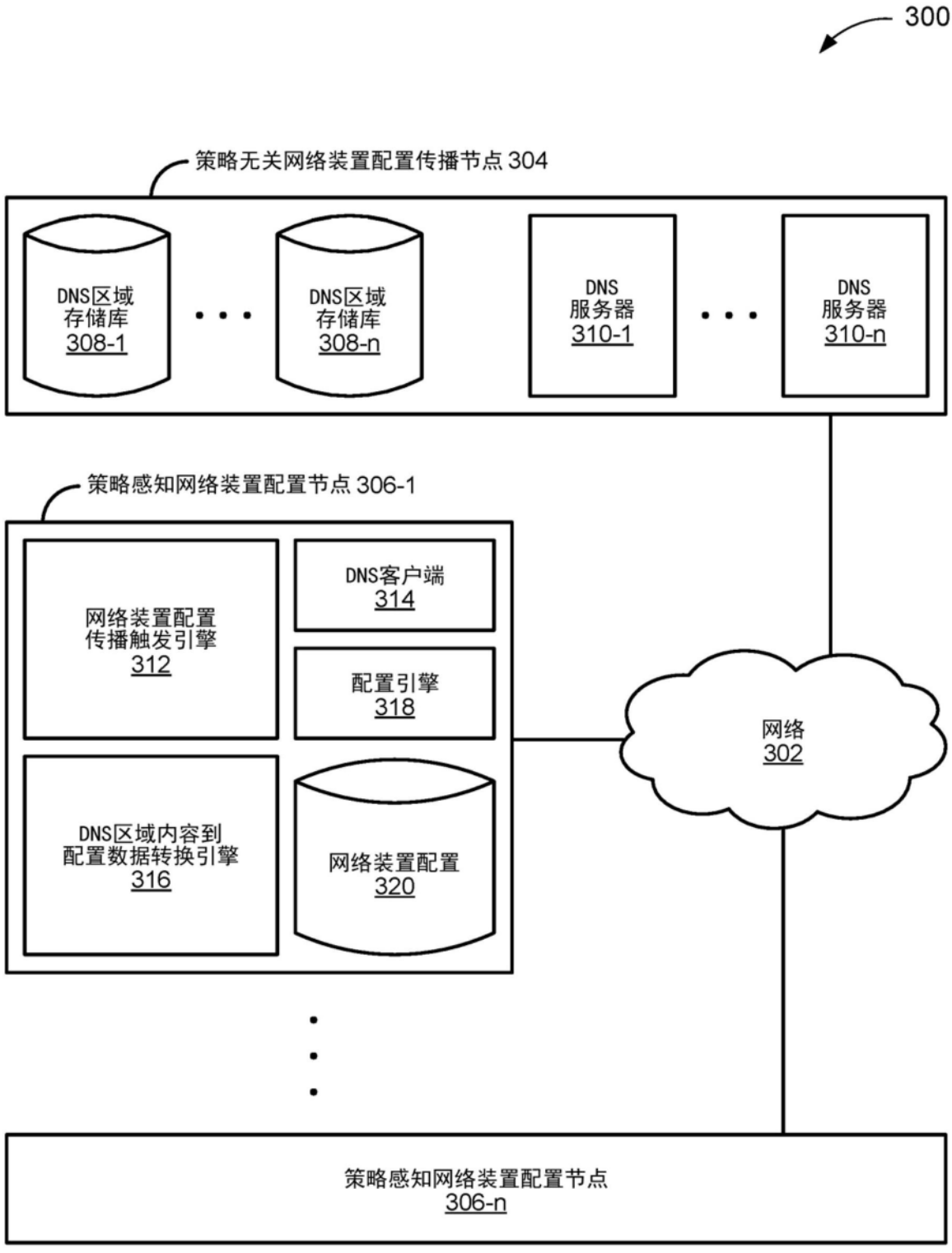

300
策略无关网络装置配置传播节点 304
DNS区域
存储库
308-1
DNS区域
存储库
308-n
DNS
服务器
310-1
DNS
服务器
310-n
策略感知网络装置配置节点 306-1
网络装置配置
传播触发引擎
312
DNS客户端
314
配置引擎
318
网络
302
DNS区域内容到
配置数据转换引擎
316
网络装置配置
320
策略感知网络装置配置节点
306-n

图3

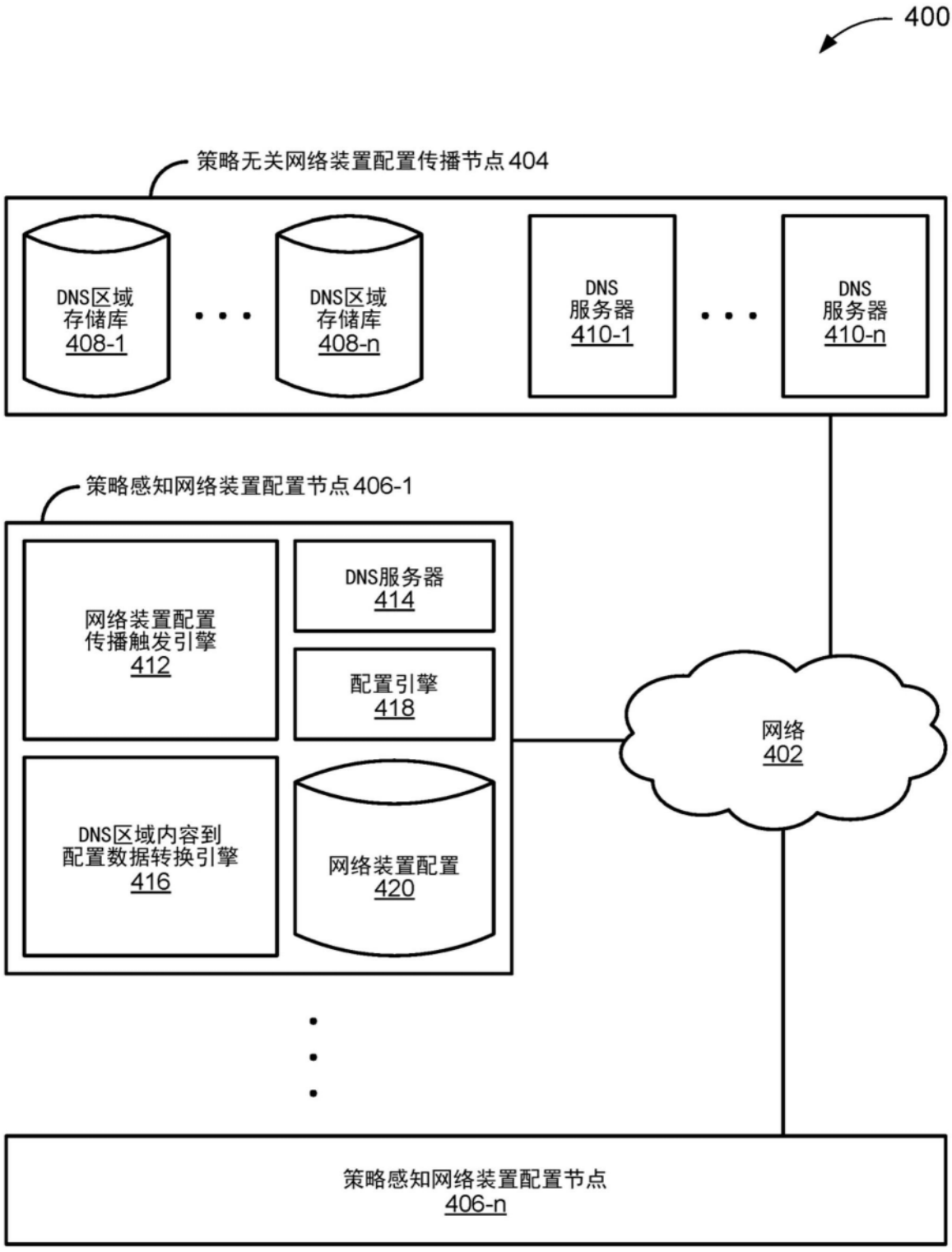

400
策略无关网络装置配置传播节点404
DNS区域存储库 408-1
DNS区域存储库 408-n
DNS服务器 410-1
DNS服务器 410-n
策略感知网络装置配置节点406-1
网络装置配置传播触发引擎 412
DNS服务器 414
配置引擎 418
DNS区域内容到配置数据转换引擎 416
网络装置配置 420
网络 402
策略感知网络装置配置节点 406-n

图4

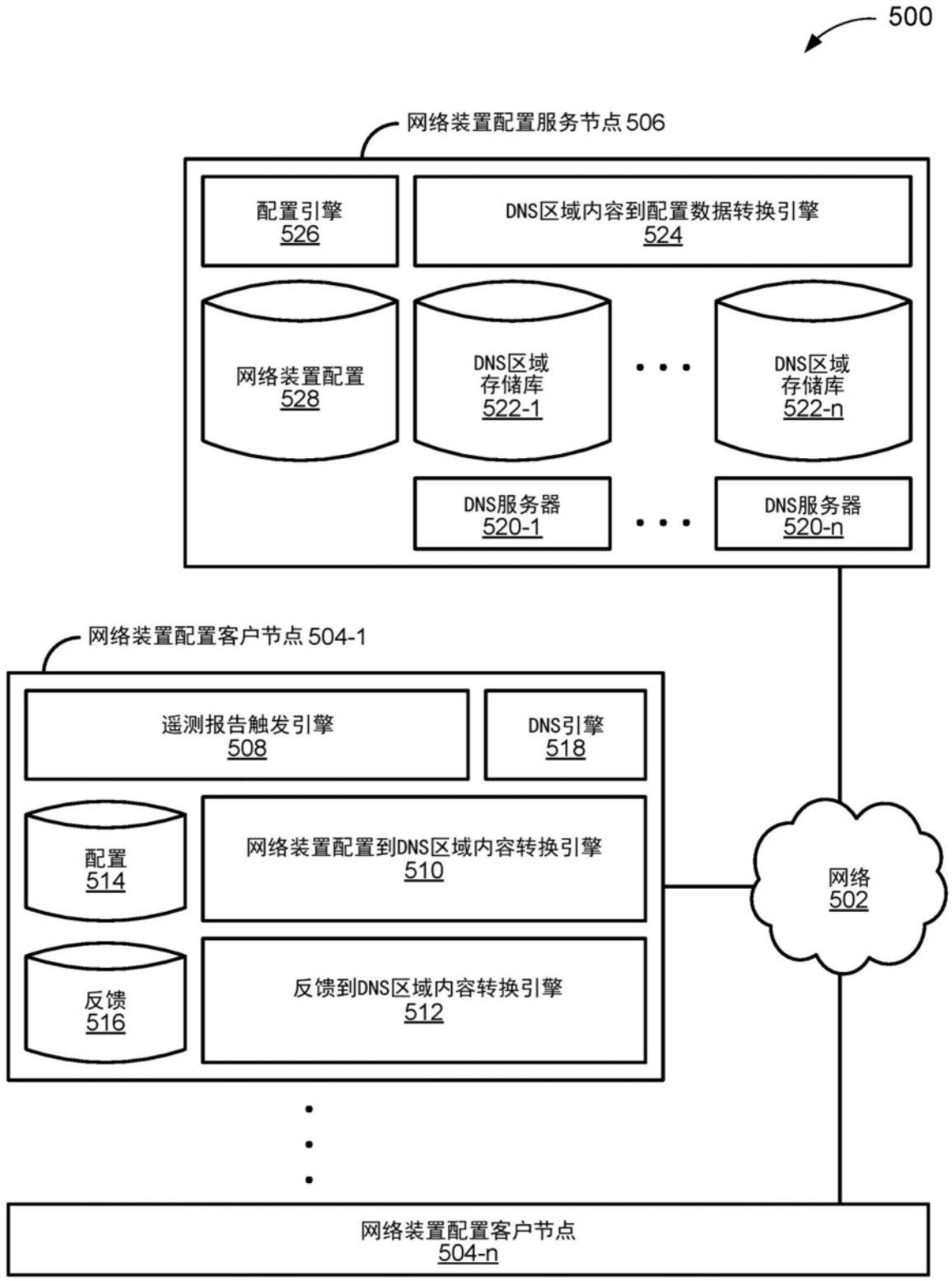

500
网络装置配置服务节点506
配置引擎
526
DNS区域内容到配置数据转换引擎
524
网络装置配置
528
DNS区域
存储库
522-1
DNS区域
存储库
522-n
DNS服务器
520-1
DNS服务器
520-n
网络装置配置客户节点504-1
遥测报告触发引擎
508
DNS引擎
518
配置
514
网络装置配置到DNS区域内容转换引擎
510
网络
502
反馈
516
反馈到DNS区域内容转换引擎
512
网络装置配置客户节点
504-n

图5

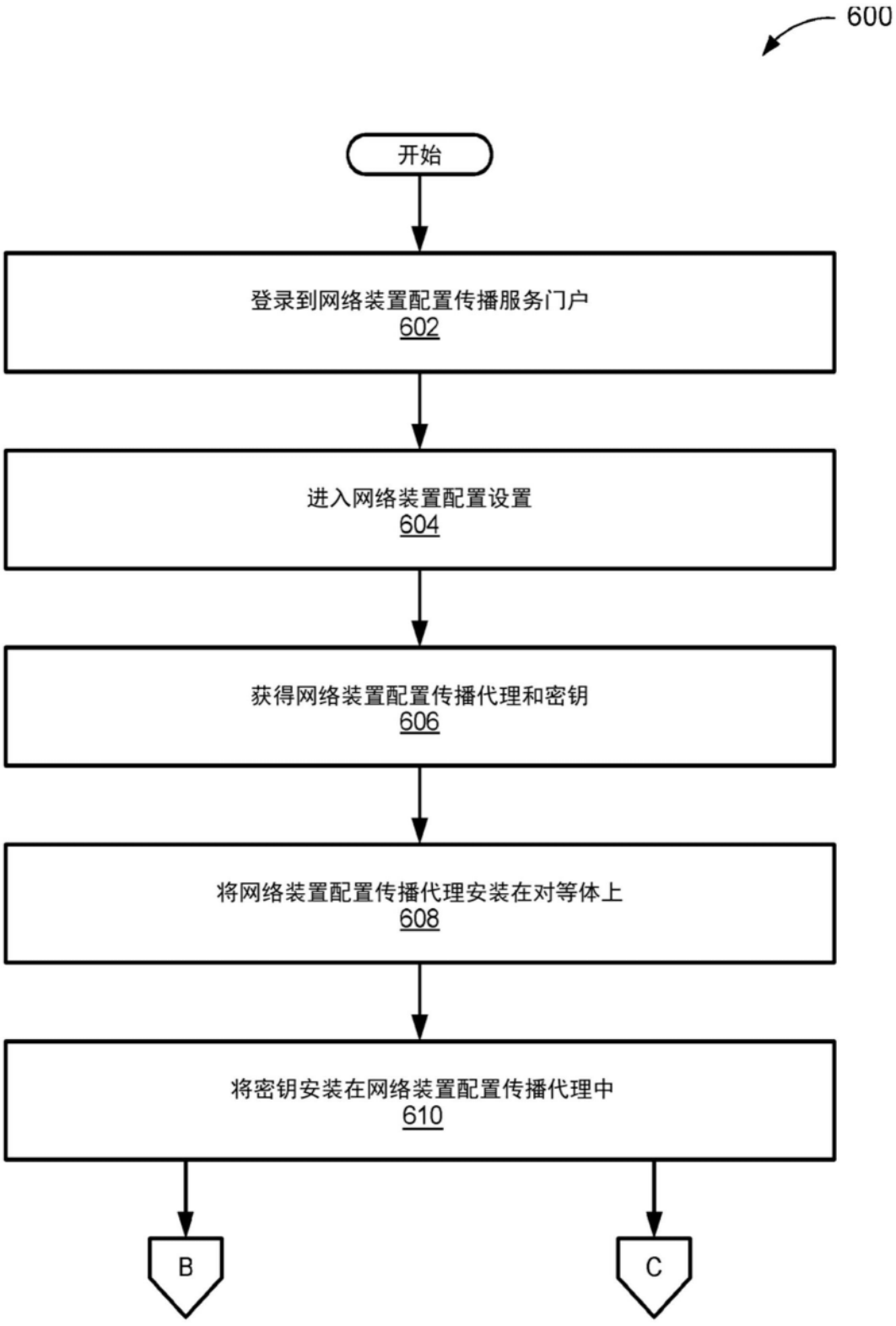

600
开始
登录到网络装置配置传播服务门户
602
进入网络装置配置设置
604
获得网络装置配置传播代理和密钥
606
将网络装置配置传播代理安装在对等体上
608
将密钥安装在网络装置配置传播代理中
610
B
C

图6A

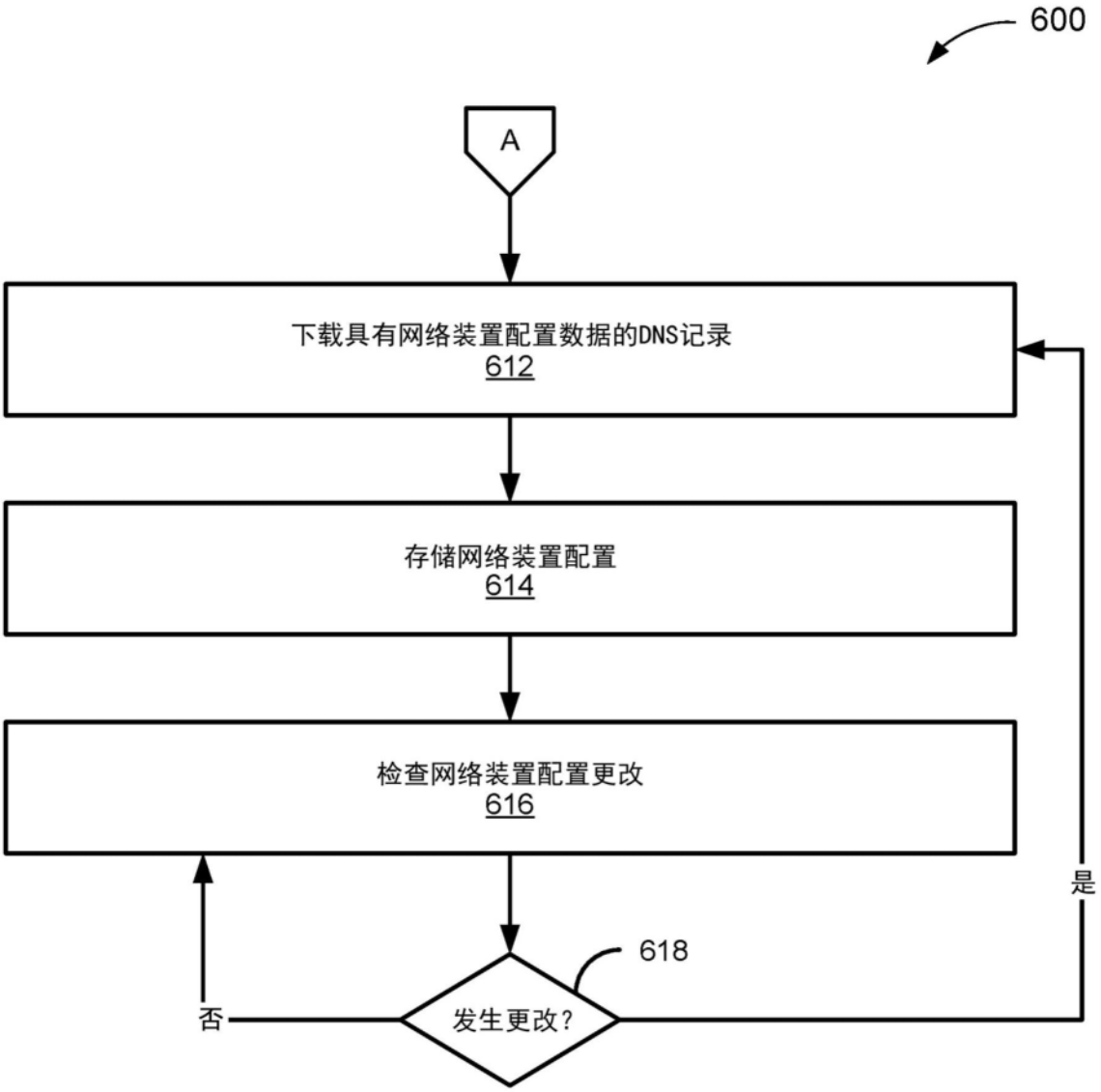

600
A
下载具有网络装置配置数据的DNS记录
612
存储网络装置配置
614
检查网络装置配置更改
616
618
发生更改?
否
是

图6B

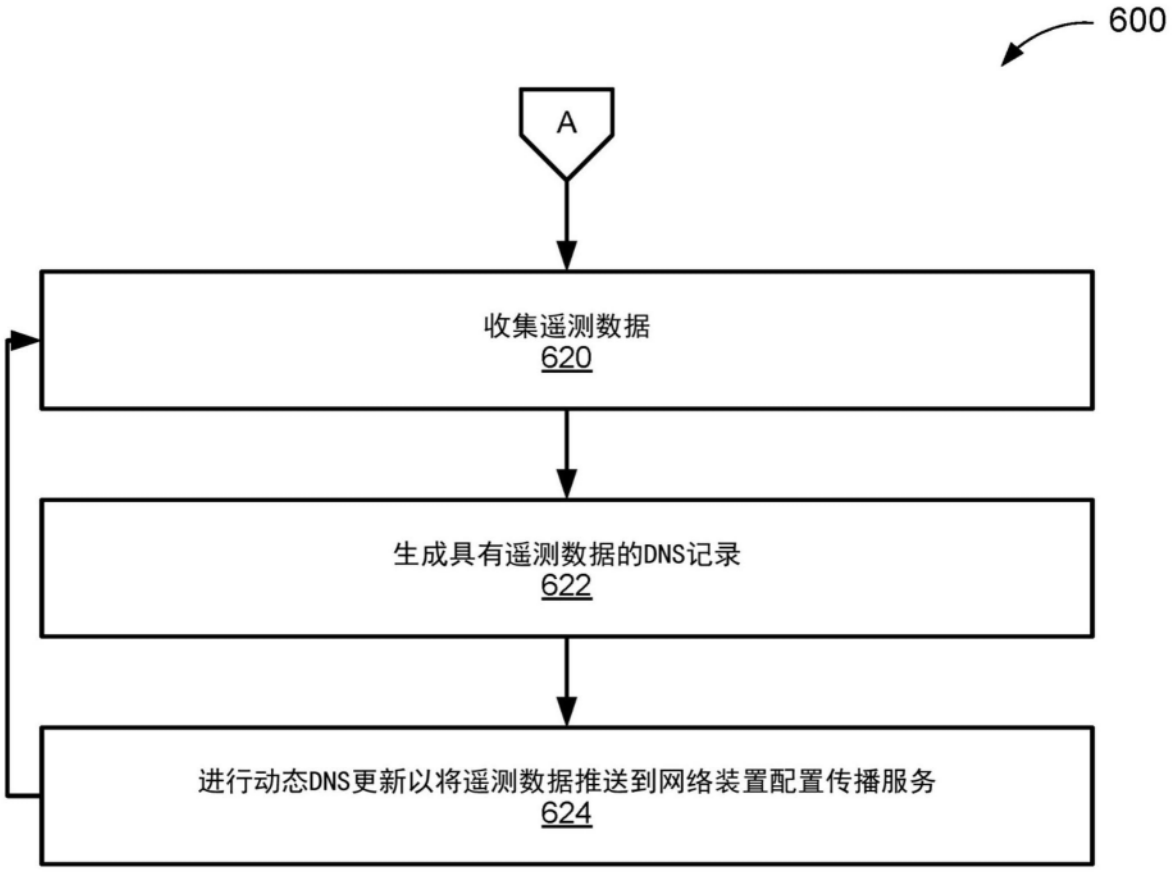

600
A
收集遥测数据
620
生成具有遥测数据的DNS记录
622
进行动态DNS更新以将遥测数据推送到网络装置配置传播服务
624

图6C

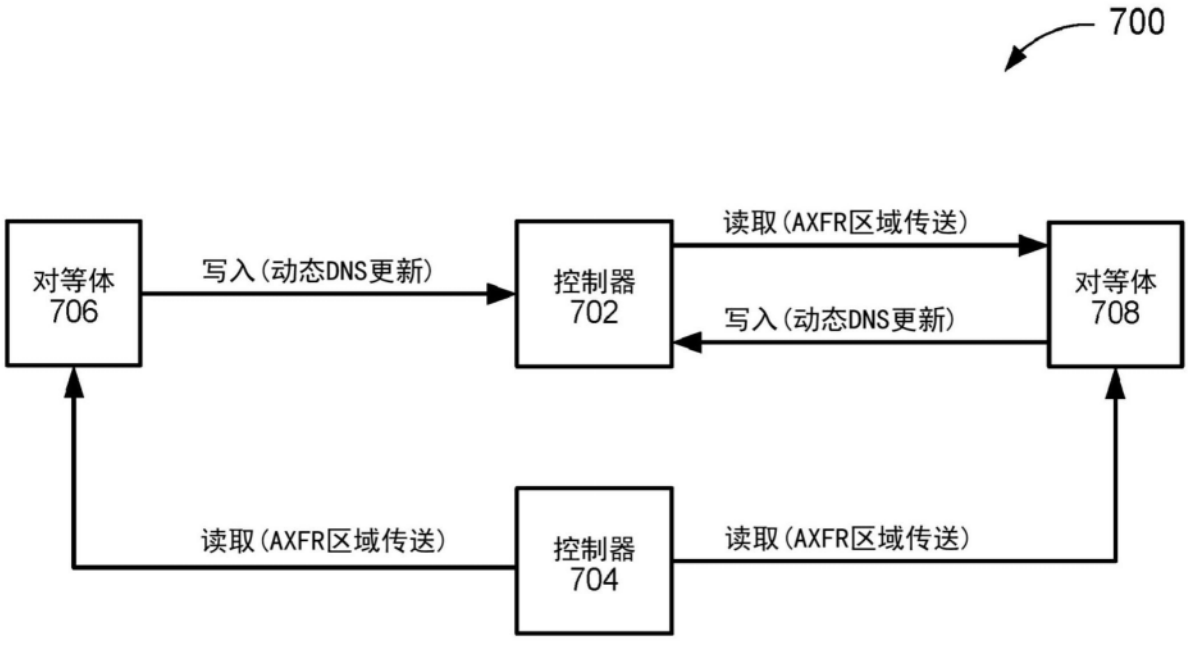

700
对等体
706
写入(动态DNS更新)
控制器
702
读取(AXFR区域传送)
写入(动态DNS更新)
对等体
708
读取(AXFR区域传送)
控制器
704
读取(AXFR区域传送)

图7

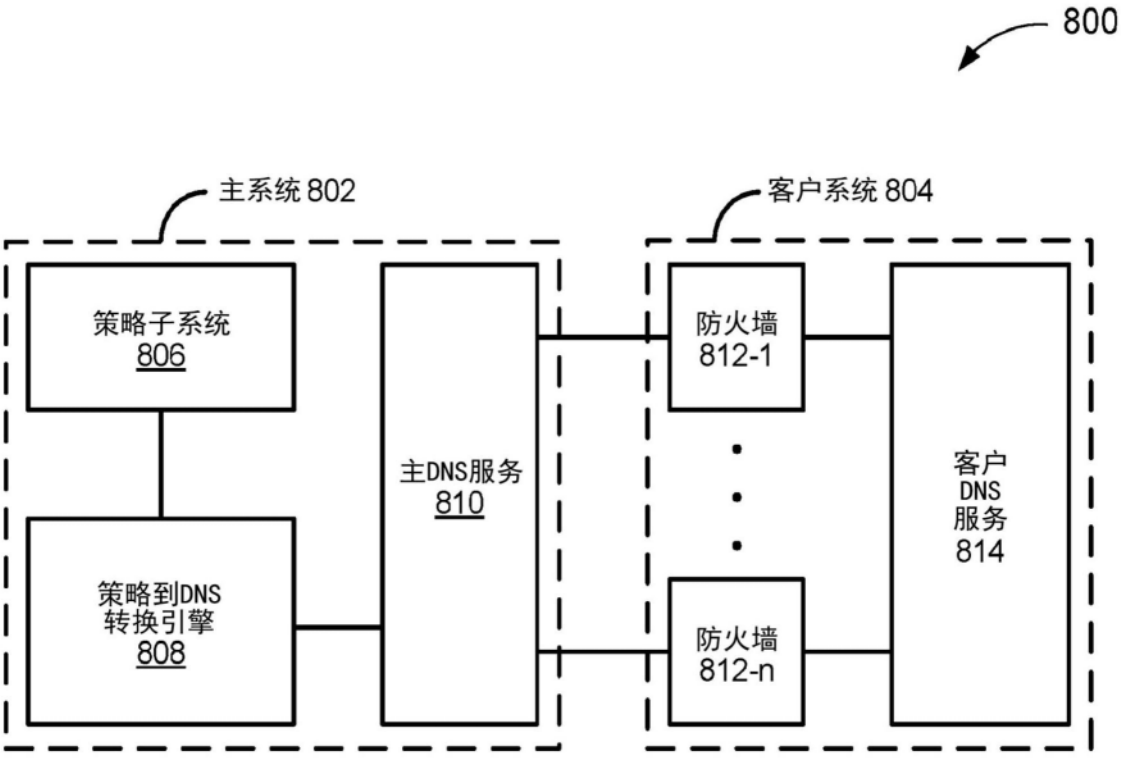

800
主系统 802
客户系统 804
策略子系统
806
策略到DNS
转换引擎
808
主DNS服务
810
防火墙
812-1
防火墙
812-n
客户
DNS
服务
814

图8

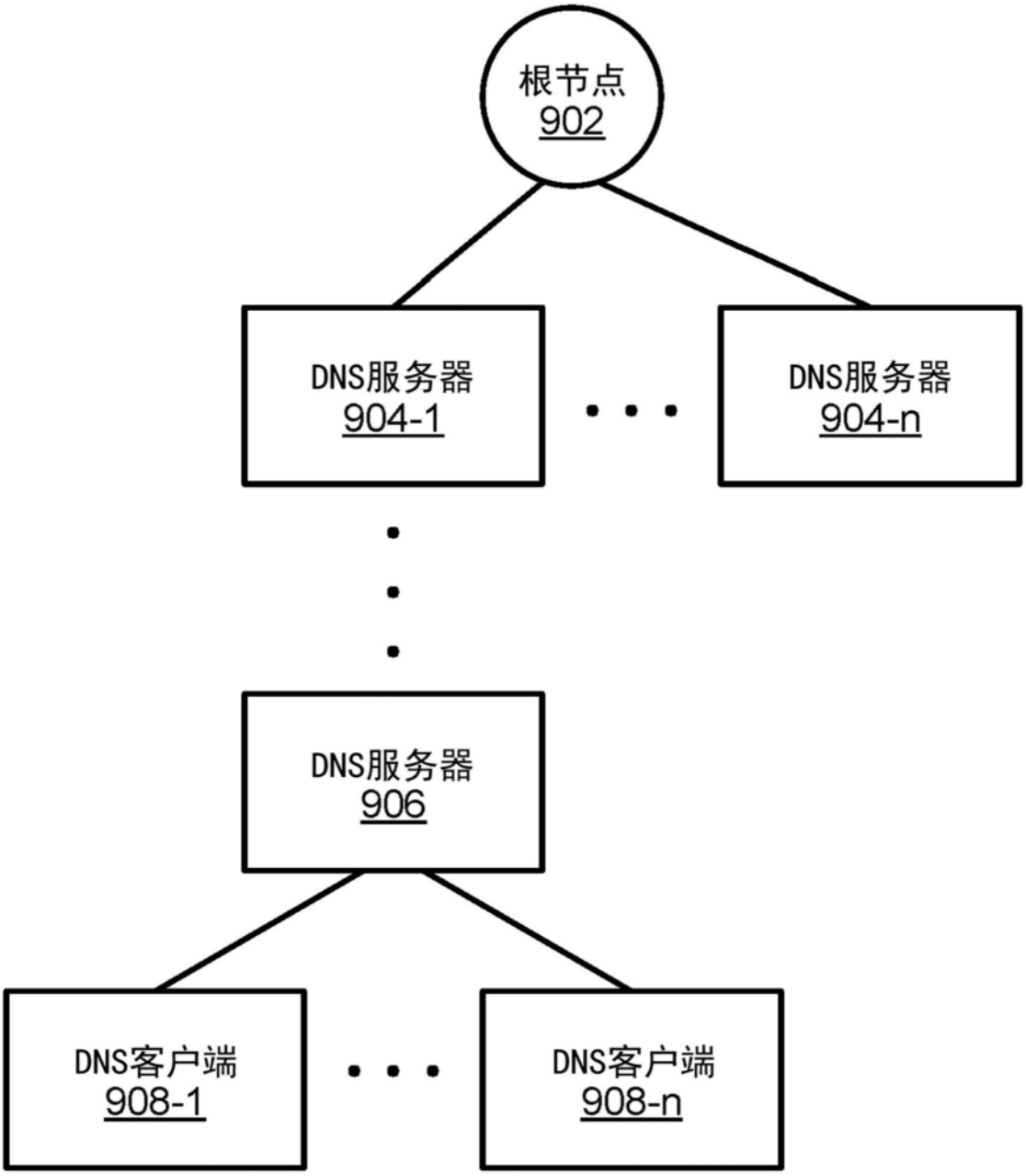

根节点
902
DNS服务器
904-1
DNS服务器
904-n
DNS服务器
906
DNS客户端
908-1
DNS客户端
908-n

图9