(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 112703717 A
(43)申请公布日 2021.04.23

(21)申请号 201980060447.9

(22)申请日 2019.09.12

(30)优先权数据
16/135,839 2018.09.19 US

(85)PCT国际申请进入国家阶段日
2021.03.16

(86)PCT国际申请的申请数据
PCT/US2019/050891 2019.09.12

(87)PCT国际申请的公布数据
WO2020/060844 EN 2020.03.26

(71)申请人 思科技术公司
地址 美国加利福尼亚州

(72)发明人 安妮卡·李·路易斯·彼得森
埃德蒙·L·王

(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 桑敏

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

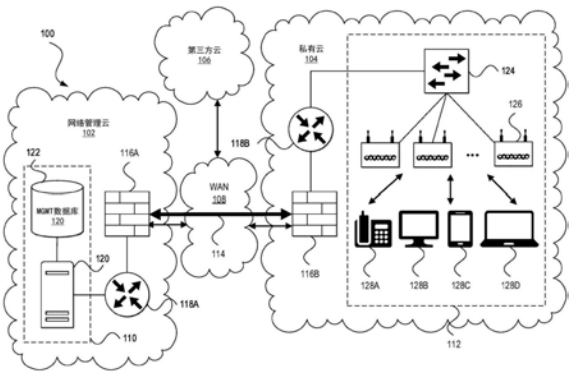
权利要求书3页 说明书14页 附图10页

(54)发明名称

跨层3网络的端点的唯一身份

(57)摘要

系统和方法提供用于确定跨L3网络的端点的唯一身份。例如,第一L3网络中的网络管理系统的第一联网设备可以从第二L3网络中的第二联网设备接收第一L3网络地址到第一L2网络地址的映射。系统可以确定第一L2网络地址与第三联网设备相关联。系统可以从第三设备接收L3地址到第二L2网络地址的映射。系统可以确定第二L2地址与端点相关联。系统可以将L3地址和第二L2地址存储作为端点的身份。系统可以基于端点的身份而使用去往/来自L3地址并与端点相关的流量来呈现端点的网络利用信息。



CN 112703717 A

1.一种计算机实现的方法,包括:

由第一层3(L3)网络中的网络管理系统的第一联网设备从第二L3网络中的第二联网设备接收L3网络地址到第一层2(L2)网络地址的第一映射;

由所述网络管理系统确定所述第一L2网络地址与第三联网设备相关联;

由所述网络管理系统从所述第三联网设备接收所述L3网络地址到第二L2网络地址的第二映射;

由所述网络管理系统确定所述第二L2网络地址与所述第二L3网络中的端点相关联;

由所述网络管理系统将所述L3网络地址和所述第二L2网络地址存储作为所述端点的身份;以及

由所述网络管理系统基于所述端点的身份而使用去往和来自所述L3网络地址并与所述端点相关的网络流量来呈现所述端点的网络利用信息。

2.根据权利要求1所述的计算机实现的方法,还包括:

基于所述端点的身份,从所述端点的所述L3网络地址解析所述端点的L2网络地址。

3.根据前述权利要求中任一项所述的计算机实现的方法,还包括:

在一段时间段中的所述端点被分配给所述L3网络地址的第一部分内,将去往所述L3网络地址的网络流量与所述端点相关联;以及

在所述时间段中的第二端点被分配给所述L3网络地址的第二部分内,将去往所述L3网络地址的第二网络流量与所述第二端点相关联。

4.根据前述权利要求中任一项所述的计算机实现的方法,还包括:

向所述第一联网设备发送第一简单网络管理协议(SNMP)消息,请求所述第一联网设备的地址解析协议(ARP)表或邻居发现协议(NDP)邻居表之一。

5.根据权利要求4所述的计算机实现的方法,还包括:

向所述第二联网设备发送第二SNMP消息,请求所述第二联网设备的ARP表或NDP邻居表之一。

6.根据权利要求5所述的计算机实现的方法,其中,所述第二SNMP消息是在所述网络管理系统接收到对所述第一SNMP消息的SNMP响应之前而发送的。

7.根据权利要求5所述的计算机实现的方法,其中,所述第二SNMP消息是在所述网络管理系统接收到对所述第一SNMP消息的SNMP响应之后而发送的。

8.根据权利要求4-7中的任一项所述的计算机实现的方法,其中,所述第一SNMP消息是以规则的时间间隔而发送的。

9.根据权利要求4-8中的任一项所述的计算机实现的方法,其中,所述第一SNMP消息是响应于所述网络管理系统在从最后一次连接起的预定时间段之后检测到来自所述L3网络地址的连接而发送的。

10.根据前述权利要求中任一项所述的计算机实现的方法,还包括:

使用所述第一L2网络地址作为查询来查询包括介质访问控制(MAC)地址的数据库以得到所述第二L3网络的联网设备。

11.根据前述权利要求中任一项所述的计算机实现的方法,还包括:

使用所述第二L2网络地址作为查询来查询包括MAC地址的数据库以得到所述第二L3网络的端点。

12.根据前述权利要求中任一项所述的计算机实现的方法,其中,所述第一映射是经由所述第一联网设备和所述第二联网设备之间的安全隧道而接收的。

13.一种系统,被配置为:

由第一层3(L3)网络中的所述系统的第一联网设备从第二L3网络中的第二联网设备接收互联网协议(IP)地址到第一介质访问控制(MAC)地址的第一映射;

确定所述第一MAC地址与第三联网设备相关联;

从所述第三联网设备接收所述IP地址到第二MAC地址的第二映射;

确定所述第二MAC地址与所述第二L3网络中的端点相关联;

将所述IP地址和所述第二MAC地址存储作为所述端点的身份;以及

基于所述端点的身份,使用去往和来自所述IP地址并与所述端点相关的网络流量来呈现所述端点的网络利用信息。

14.根据权利要求13所述的系统,还被配置为:

基于所述端点的身份,从所述端点的所述IP地址解析所述端点的MAC地址。

15.根据权利要求13-14中的任一项所述的系统,还被配置为:

在一段时间段中的所述端点被分配给所述IP地址的第一部分内,将去往所述IP地址的所述网络流量与所述端点相关联;以及

在所述时间段中的第二端点被分配给所述IP地址的第二部分内,将去往所述IP地址的第二网络流量与所述第二端点相关联。

16.根据权利要求13-15中的任一项所述的系统,还被配置为:

使用所述第一MAC地址作为查询来查询包括MAC地址的数据库以得到所述第二L3网络的联网设备。

17.一种计算机可读存储介质,其中存储有指令,这些指令在由系统的一个或多个处理器执行时使所述系统:

由第一层3(L3)网络中的所述系统的第一联网设备从第二L3网络中的第二联网设备接收互联网协议(IP)地址到第一介质访问控制(MAC)地址的第一映射;

确定所述第一MAC地址与第三联网设备相关联;

从所述第三联网设备接收所述IP地址到第二MAC地址的第二映射;

确定所述第二MAC地址与所述第二L3网络中的端点相关联;

将所述IP地址和所述第二MAC地址存储作为所述端点的身份;以及

基于所述端点的身份,使用去往和来自所述IP地址并与所述端点相关的网络流量来呈现所述端点的网络利用信息。

18.根据权利要求17所述的计算机可读存储介质,还包括指令,这些指令当被执行时还使所述系统:

向所述第一联网设备发送第一简单网络管理协议(SNMP)消息,请求所述第一联网设备的地址解析协议(ARP)表或邻居发现协议(NDP)邻居表之一;以及

向所述第二联网设备发送第二SNMP消息,请求所述第二联网设备的ARP表或NDP邻居表之一。

19.根据权利要求18所述的计算机可读存储介质,其中,所述第二SNMP消息是在所述系统接收到对所述第一SNMP消息的SNMP响应之前而发送的。

20.根据权利要求18-19中的任一项所述的计算机可读存储介质,其中,所述第一SNMP消息是以规则的时间间隔而发送的。

跨层3网络的端点的唯一身份

[0001] 相关申请的交叉引用

[0002] 本申请要求于2018年9月19日提交的题为“UNIQUE IDENTITIES OF ENDPOINTS ACROSS LAYER 3NETWORKS(跨层3网络的端点的唯一身份)”的美国非临时专利申请第16/135,839号的权益和优先权,其内容在此明确地通过引用整体并入。

技术领域

[0003] 本公开的主题一般地涉及电信网络领域,并且更具体地涉及用于确定跨层3网络的端点的唯一身份的系统和方法。

背景技术

[0004] 云联网(有时也称为基于云的联网、软件定义的广域联网(SD-WAN)、或云WAN)描述了私有网络(例如,第一层3(L3)网络)使用WAN或基于互联网的接入技术从外部网络提供商(例如,第二L3网络)访问网络资源。云联网可提供集中式管理和控制,而无需本地部署(on-premise)网络控制器设备或覆盖网络管理系统的成本和复杂性。云联网还可以涉及使用云中的集中式管理来管理分布式无线接入联网设备或分支机构联网设备。云联网可以允许经由可以驻留在数据中心的集中式管理功能和WAN连接来创建和管理安全的私有网络。云网络还可以使连接性、安全性、管理和控制功能能够被推送到云中并作为服务交付。然而,当前的云网络实现方式遭受各种缺点,例如关于跨L3网络的端点的可见性的限制。

附图说明

[0005] 为了提供对本公开及其特征和优点的更完整理解,参考以下结合附图的描述,其中:

[0006] 图1示出了根据实施例的网络的示例;

[0007] 图2示出了根据实施例的用于基于云的网络管理系统的控制器的示例;

[0008] 图3A-3D示出了根据一些实施例的用于确定跨L3网络的端点的唯一身份的过程的流程图的示例;

[0009] 图4示出了根据实施例的用于管理跨L3网络的端点的唯一身份的过程的示例;

[0010] 图5示出了根据实施例的图形用户界面的示例,该图形用户界面用于使用与跨L3网络的端点的唯一身份相关的网络流量来呈现该端点的网络利用信息;

[0011] 图6示出了根据实施例的联网设备的示例;

[0012] 图7A和7B示出了根据一些实施例的系统的示例。

具体实施方式

[0013] 以下阐述的详细描述旨在作为实施例的各种配置的描述,而不旨在代表可以实践本公开的主题的唯一配置。附图并入本文并构成详细描述的一部分。为了提供对本公开的主题的更透彻的理解,详细描述包括特定细节。然而,将显而易见的是,本公开的主题不限

于本文阐述的具体细节，并且可以在没有这些细节的情况下实践。在一些实例中，以框图形式示出了结构和组件，以避免使本公开的主题的概念不清楚。

[0014] 概述

[0015] 系统和方法提供用于确定跨层3(L3)网络的端点的唯一身份。在实施例中，第一L3网络(例如，云提供商网络)中的网络管理系统的第一L3联网设备(例如，交换机、路由器、网关等)可以从第二L3网络(例如，私有网络)中的第二联网设备接收L3网络地址(例如，互联网协议(IP)地址)到第一层2(L2)网络地址(例如，介质访问控制(MAC)地址)的第一映射。网络管理系统可以确定第一L2网络地址与第二L3网络中的第二联网设备相关联。网络管理系统可以请求并接收L3网络地址到第二L2网络地址的第二映射。网络管理系统可以确定第二L2网络地址与第二L3网络的端点相关联。网络管理系统可以将第一L3网络地址和第二L2网络地址存储作为端点的唯一身份。网络管理系统可以基于端点的唯一身份，使用去往/来自L3网络地址并与端点相关的网络流量来监视并呈现端点的网络利用信息。

[0016] 示例实施例

[0017] 一些网络管理系统可以通过L2网络地址(例如MAC地址)来识别端点，例如通过分析流经网络网关的流量、网关的路由表、ARP表、NDP邻居表、或类似的L3-L2网络地址映射信息。但是，由于有多少个L3联网设备运行的方式，这种方法可能无法准确地识别端点。例如，L3联网设备可以将接收到的去往/来自下游或下一跳联网设备的IP分组的L2网络地址改变为其自己的L2网络地址。因此，上游网络或联网设备可以将端点的IP地址与L3联网设备的MAC地址相关联。这可能导致上游网络或联网设备将端点流量识别为L3联网设备的流量。

[0018] 一些网络管理系统可以通过L3网络地址来识别端点。由于许多L3网络可以在一段时间内将相同的L3网络地址分配给多个端点，因此该方法也可能存在缺陷。例如，无线局域网(WLAN)、企业网络、物联网(IoT)环境、IP语音(VoIP)系统、以及类似的网络可以包含许多联网设备和端点，但可能仅具有有限数量的IP地址。这些网络可以为端点动态分配IP地址，并且可以为多个设备分配相同的IP地址。上游网络或联网设备可以将端点流量识别为单个端点的流量，但是部分或全部流量实际上可能源自另一个端点或多个其他端点。

[0019] 端点的正确识别对于网络管理可能至关重要。例如，网络保证、服务质量(QoS)、分析等可能依赖于将端点彼此准确区分以及将端点与联网设备进行准确区分。作为另一个示例，可能无法实现基于端点的网络策略，例如白名单规则(例如，仅当存在允许访问的策略时才允许端点访问的网络策略)或黑名单规则(例如，除非存在禁止访问的策略否则允许端点访问的网络策略)，这些策略使用端点标识符表示，但是对这些标识符的准确性没有信心。作为又一个示例，网络拓扑发现可能要求端点具有不同的身份。

[0020] 本公开的各种实施例可以通过利用IP地址和MAC地址的映射唯一地识别端点来克服现有技术的上述和其他缺陷。网络可以维护IP-MAC地址映射的数据库，以表示指定时间段内端点的规范身份。网络可以连续更新数据库以反映端点的当前状态。各种网络管理应用和服务(例如保证、QoS、分析、安全性、网络拓扑映射等)可以依赖于IP-MAC地址映射信息来准确识别端点。

[0021] 图1示出了在其中部署主题技术的网络环境100的示例。应当理解，对于网络环境100和本文讨论的任何环境，在相似或替代配置中可以存在附加或更少的节点、设备、链路、网络、或组件。本文中还设想了具有不同数量和/或类型的端点、网络、节点、云组件、服务

器、软件组件、设备、虚拟或物理资源、配置、拓扑、服务、器具、部署、或联网设备的示例实施例。此外，网络环境100可以包括可由端点或租户访问和利用的任何数量或类型的资源。本文提供的图示和示例是为了清楚和简单起见。

[0022] 网络环境100可以包括网络管理云102；私有云104；第三方云106，用于提供各种第三方内容和服务，例如电子邮件、媒体内容(例如，视频、音乐、游戏等)、在线银行和社交网络等；以及互连网络管理云102、私有云104和第三方云106的WAN 108(例如互联网)。网络管理云102可以托管用于管理私有云104中的无线LAN(WLAN)112的网络管理系统110。云托管的网络管理系统110可被配置为管理各种设备在LAN(例如WLAN 112)中和/或跨越一个或多个虚拟LAN(VLAN)的地理分布部分的配置和操作。

[0023] 可以经由网络管理云102中的第一安全设备116A和第一L3联网设备118A以及私有云104中的第二安全设备116B和第二L3联网设备118B(分别统称为安全设备116和L3联网设备118)在网络管理云102和私有云104之间建立安全连接114。除了建立安全连接114，安全设备116还可以提供其他联网服务，例如虚拟私有网(VPN)集中、防火墙、目录服务、证书授权服务、策略管理、入侵检测和预防、负载平衡、WAN加速、内容过滤等。在一些实施例中，Cisco Meraki® MX设备可以作为安全设备116操作。在一些实施例中，Cisco Catalyst®、Cisco Nexus®、和/或Cisco Meraki® MS交换机可以作为L3联网设备118操作。另一些实施例可以利用多个供应商来提供安全设备116和L3联网设备118的功能。

[0024] 网络管理系统110和WLAN 112的设备可以使用安全连接114来交换管理数据(例如，配置、统计或监视数据)。安全连接114可以以各种方式来实现，诸如利用VPN或L2隧道协议。在一些实施例中，可以使用开放式VPN(例如，OpenVPN)覆盖或基于IP安全性(IPSec)VPN的L3网络扩展来提供安全连接114。在其他实施例中，安全传输层(即，L4)隧道可以用作安全设备116之间的安全连接114，例如通过跨WAN 108利用传输层安全性(TLS)、数据报TLS(DTLS)、安全套接字层(SSL)等。

[0025] 安全连接114可以利用WAN 108的各个部分。例如，经由安全连接传输的分组可以被标记和/或包含报头字段，这些报头字段使得能够优先化WAN 108的至少一些部分上的安全隧道分组。在一些示例实施例中，安全隧道分组的优先化可以包括在网络管理系统110和WLAN 112之间使用私有专用路由路径，以减少时延和/或提高可靠性。

[0026] 云托管的网络管理系统110可以包括管理数据库(MGMT)120和网络管理服务器122。网络管理服务器122可以管理云操作、端点通信、服务供应、网络配置和监视等。管理数据库120可以存储与WLAN 112相关的配置信息、统计、监视信息和其他管理数据。在一些实施例中，Cisco Meraki®云网络平台可以作为云托管的网络管理系统110操作。

[0027] WLAN 112可以包括接入交换机124(例如，L2/L3联网设备)、接入点126和端点，诸如台式电话128A、台式计算机128B、智能电话128C和膝上型计算机128D(统称为端点128)。端点128还可以包括服务器、平板电脑、可穿戴设备、安全相机、物联网(IoT)设备、或其他能够在一定距离上以电子方式发送和接收音频、视频和/或其他数据的设备。每个端点128可以包括一个或多个处理器、一种或多种类型的存储器、显示器、和/或其他用户接口组件，例如键盘、触摸屏显示器、鼠标、触控板、数码相机、和/或为端点添加功能的任意数量的外围设备或组件。端点128还能够进行协议处理、调制、解调、数据缓冲、功率控制、路由、切换、时

钟恢复、放大、解码、和/或错误控制。

[0028] 接入交换机124可以用作L3联网设备118B和接入点126之间的LAN接口。接入点126可以为端点128提供在WLAN 112中的网络访问。安全设备116B、L3联网设备118B、接入交换机124和接入点126可以被配置为根据由网络管理系统110提供的规则、配置指令、软件和/或固件更新进行通信和操作。在一些实施例中，安全设备116B、L3联网设备118B、接入交换机124和接入点126的功能可以集成到单个物理设备中，例如Cisco Meraki® MR接入点。其他实施例可以将网络的不同功能元件进行组合，例如安全设备和L3联网设备被集成到单个物理设备(如Cisco Meraki® MX设备)；L3路由器和L2交换机被集成到单个物理设备(例如Cisco Meraki® MS交换机)；L3路由器、L2交换机和无线接入点被集成到单个物理设备(例如Meraki® MR接入点)；等等。其他实施例可以针对网络的每个功能元件利用多个供应商。

[0029] 图2示出了用于云网络管理系统(例如，云网络管理系统110)的网络控制器210的示例。本领域普通技术人员将理解，对于本公开中所讨论的网络控制器210和任何系统，在相似或替代配置中可以存在附加或更少的组件。本公开中提供的图示和示例是为了简洁和清楚。其他实施例可以包括不同数量和/或类型的元件，但是本领域的普通技术人员将理解，这种变型不脱离本公开的范围。

[0030] 网络控制器210可以远程地托管在管理网络(例如，网络管理云102)中，并且可以用作用于为云网络服务的提供商的客户管理和控制管理网络和一个或多个私有网络(例如，私有云104)的元件(包括联网设备(例如，安全设备116B、L3联网设备118B、接入交换机124、接入点126等)和/或端点(例如，端点128))的网络管理系统。例如，网络控制器210可以管理各种云服务，例如在管理网络中供应云资源，配置和更新云资源，监视云资源，实施针对云资源的高可用性和故障转移，强制执行针对云资源的安全性和合规性，等等。网络控制器210还可以向端点发送网络数据以及从端点接收网络数据以促进端点的配置；监视私有网络和私有网络的联网元件(例如安全连接(例如，安全连接114)、私有网络网关(例如，安全设备116B)、路由器(例如，L3联网设备118A)、L2/L3交换机(例如，接入交换机124)和接入点(例如，接入点126)、以及其他元件)的状态信息；以及管理私有网络和私有网络的元件。

[0031] 网络控制器210可以包括若干组件或模块，例如通信接口230、管理层232、用户接口层234、数据层220、网络层236、端点身份(ID)服务238和数据层220。这些模块可以实现为硬件、固件和/或软件组件。虽然图2示出了网络控制器210的各种组件的示例配置，但是本领域技术人员将理解，网络控制器210的组件或本文描述的任何设备可以以多种不同的方式来配置并且可以包括任何其他类型和数量的组件。例如，管理层232和网络层236可以属于一个软件模块或多个单独的模块。其他模块也可以组合成更少的组件和/或进一步划分成更多的组件。

[0032] 通信接口230可以允许网络控制器210与端点以及任何其他设备或网络进行通信。通信接口230可以包括网络接口卡(NIC)，并且可以包括有线和/或无线能力。通信接口230可以允许网络控制器210从其他设备和网络发送和接收数据。网络控制器210可以包括用于冗余或故障转移的多个通信接口。例如，网络控制器210可以包括用于连接冗余的双NIC。

[0033] 管理层232可以包括执行管理操作的逻辑。例如，管理层232可以包括允许网络控制器210的各种组件进行接口并一起工作的逻辑。管理层232还可以包括逻辑、功能、软件和

过程，以允许网络控制器210进行监视、管理、控制和治理私有网络中的设备、私有网络中的应用、提供给设备的服务、或任何其他组件或过程。管理层232可以包括用于操作网络控制器210并执行由网络控制器210配置的特定服务的逻辑。管理层232还可以启动、启用或发起网络控制器210的其他实例。在一些实施例中，管理层232还可以为管理网络、网络控制器210、私有网络、端点、和/或任何其他设备或组件提供认证和安全服务。此外，管理层232可以管理节点、资源、设置、策略、协议、通信等。

[0034] 用户接口层234可以提供前端，端点可以利用该前端来访问或使用云服务。例如，用户接口层234可以提供基于web的仪表板、桌面应用、移动应用、或其他合适的接口，管理员可以在其中配置受云管理的端点或私有网络，提供用户偏好，指定策略，输入数据，查看统计，配置交互或操作等。用户接口层234还可提供可见性信息，例如私有网络或端点的视图。例如，用户接口层234可以提供私有网络的状态或状况、发生的操作、服务、性能、拓扑或布局、特定联网设备、实现的协议、运行的进程、错误、通知、警报、网络结构、正在进行的通信、数据分析等的视图。

[0035] 在一些实施例中，用户接口层234可以为用户提供图形用户界面(GUI)，以监视私有网络、设备、统计、错误，通知等，并通过GUI进行修改或设置更改。GUI可以描绘图表、列表、表格、地图、拓扑、符号、结构、或任何图形对象或元素。此外，GUI可以使用颜色、字体、形状、或任何其他特性来描绘得分、警报或状况。在实施例中，用户接口层234还可以处理用户或端点请求。例如，管理员或端点可以通过用户接口层234输入服务请求。

[0036] 网络层236可以执行诸如网络寻址之类的网络计算，或者诸如自动VPN配置或流量路由之类的联网服务或操作。网络层236还可以执行过滤功能、交换功能、故障转移功能、高可用性功能、网络或设备部署功能、资源分配功能、消息收发功能、流量分析功能、端口配置功能、映射功能、分组操纵功能、路径计算功能、循环检测、成本计算、错误检测、或以其他方式操纵数据或联网设备。在一些实施例中，网络层236可以处理来自其他网络或设备的联网请求，以及在设备之间建立链接。在一些实施例中，网络层236可以执行排队、消息收发和协议操作。

[0037] 数据层220可以包括任何数据或信息，例如管理数据、统计、设置、偏好、配置文件数据、日志、通知、属性、配置参数、端点信息、网络信息等。例如，网络控制器210可以从端点收集网络统计并将统计存储作为数据层220的一部分。数据层220还可以包括性能和/或配置信息，并且网络控制器210可以使用数据层220来执行对端点的管理或服务操作。数据层220可以存储在网络控制器210上的存储器或存储设备、连接到网络控制器210的单独的存储设备、或与网络控制器210通信的远程存储设备上。

[0038] 数据层220可以包括用于盘点网络设备的设备数据库240。设备数据库240可以存储设备信息，例如设备的IP地址、MAC地址、名称、类型、制造商、型号、序列号、状态(例如，在线或离线)、一个或多个网络策略、功能、Cisco®发现协议和/或链路层发现协议(LLDP)信息、信道宽度、它所连接到的接入点、网络首次看到的时间戳、网络最后看到的时间戳、描述、元数据标签、操作系统、端口、服务集标识符(SSID)、网络使用情况(例如，按照字节、分组;总使用量或每个接口)、用户、VLAN、地理围栏状态、登记日期、隔离状态等。

[0039] 在一些实施例中，设备数据库240可以被划分为包括联网设备数据库242和端点数据库244。联网设备数据库242可以快速识别给定的MAC地址是否对应于网络的已知联网设

备。联网设备数据库242可以以扩展唯一标识符(EUI)-48格式(例如,MM:MM:MM:SS:SS:SS)或EUI-64格式(例如,MM:MM:MM:SS:SS:SS:SS:SS)存储MAC地址,其中前3个字节可以代表互联网标准机构分配给制造商的组织唯一标识符(OUI),其余字节可以代表制造商分配的设备序列号。在一些实施例中,联网设备数据库242可以被实现为数据集市(例如,被配置为提供对数据子集的更快访问的数据库的子集)或联网设备信息的其他优化视图。在这样的实施例中,联网设备数据库242可以附加地或替代地包括用于解析给定的MAC地址是否对应于已知联网设备的规则或操作。在一些实施例中,可以使用内容可寻址存储器(CAM)来实现联网设备数据库242。端点数据库244可以通过IP地址和MAC地址的组合来唯一地识别网络中的端点。端点数据库244可以代表端点身份的规范来源。

[0040] 端点ID服务238可以通过IP地址和MAC地址的映射来跟踪端点的唯一标识。端点ID服务238可以周期性地更新端点数据库244,以确保数据库反映网络的当前状态。在一些实施例中,更新可以以规则的时间间隔发生,例如每秒钟、分钟、小时、或其他合适的时间标度。替代地或附加地,更新可以是由事件驱动的,例如当联网设备断开连接并重新连接到网络时,或者当在网络中首次检测到或自从在网络中最后检测到IP地址以来的预定时间段之后检测到IP地址时。

[0041] 端点ID服务238可以利用各种技术来管理端点在网络中的唯一身份。例如,端点ID服务238可以取得联网设备的下游设备(例如,其他联网设备或端点)的IP-MAC地址映射。如果联网设备的下游设备是与已知联网设备相对应的MAC地址(例如,与联网设备数据库242中的MAC地址或规则匹配),则端点ID服务238可使该下游设备取得针对它的每个下游设备的IP-MAC地址映射,依此类推,直到获取MAC地址的真实端点为止。端点ID服务238可以利用各种协议和技术来从联网设备及其下游设备取得IP-MAC地址映射信息,例如简单网络管理协议(SNMP)、邻居发现协议(NDP)、互联网控制消息协议(ICMP)、地址解析协议(ARP)、动态主机配置协议(DHCP)、CDP、LLDP、行业标准发现协议(ISDP)、网络配置协议(NETCONF)/更下一代(YANG)、gRPC远程过程调用(gRPC)、安全外壳(Secure Shell)、Telnet、OpenFlow™、或类似的协议和技术。

[0042] 表1列出了端点ID服务238为网络的给定联网设备找到端点的真实MAC地址的一种可能方式的伪代码示例。

[0043] 表1:用于管理IP-MAC地址映射以唯一识别端点的伪代码示例

```
manageEndpointIdentities(networkDevice A) {
   for each downstreamDevice B of A {
      // get IP address observed by B
      ipAddr = B.getIpAddress();

      // get MAC address observed by B
      macAddr = B.getMacAddress();
      if (ipAddr is in A's network &&
          macAddr != known network device in A's network) {
         // macAddr is true endpoint MAC address;
         // Update Endpoint DB with IP-MAC mapping
         updateEndpointDB(ipAddr, macAddr);
      } else {
         // macAddr is associated with networking device;
         // Recursion to find true endpoint MAC address
         manageEndpointIdentities(B);
      }
   }
}
```

[0044]

[0045] 图3A-3D示出了用于确定跨L3网络的端点的唯一身份的过程的流程图的示例。图3A和3B示出了可以例如由网络管理系统(例如,网络管理系统110)集中管理的过程的示例。图3C和3D示出了分散过程的示例,在分散过程中,联网设备本身可以作为网络管理系统操作。普通技术人员将理解,对于本文所讨论的任何过程,除非另有说明,否则在各种实施例的范围内可以有以相似或替代顺序或并行执行的附加、较少或替代步骤。

[0046] 图3A示出了用于确定跨L3网络的端点(例如,端点128)的唯一身份的集中管理和集中控制的过程300。在过程300中,可以在网络管理系统110可以确定端点128的唯一身份之前发生某些操作。例如,端点128可以经由802.11关联302连接到无线接入点(例如,接入点126),其中端点128和接入点126交换一系列管理帧,以使端点128进入已验证和关联的状态。

[0047] 响应于端点128与接入点126之间的802.11关联302,一个或多个联网设备可以执行L3-L2网络地址映射信息(例如DHCP、ARP、或NDP邻居表等)的更新304。例如,L3联网设备118可以利用端点128的IP地址到接入交换机124的MAC地址的映射来更新其ARP表;可以作为L3交换机操作的接入交换机124可以利用端点128的IP地址到接入点126的MAC地址的映射来更新其ARP表;以及也可以作为L3交换机操作的接入点126可以利用端点128的IP地址到端点的MAC地址的映射来更新其ARP表。

[0048] 例如,如果L3联网设备118B提供用于将L3网络地址分配给端点的动态主机配置协议(DHCP)服务,并且首次或在预定时间段(例如,DHCP租用时间)之后将L3网络地址分配给连接到网络的端点128,则可以发生更新。对于DHCP服务从端点128到L3联网设备118B的路由可以将接入交换机124、接入点126和L3联网设备118B识别为下一跳,并且可以使联网设备更新其ARP表、NDP邻居表、或其他IP-MAC地址映射信息。

[0049] 作为另一个示例,接入点126可以作为端点128的默认网关操作。端点可以尝试首

次与另一个网络中的主机进行通信，并向接入点126发送ARP或NDP广播消息以获取主机的IP地址。路由到外部主机可以将L3联网设备118B和接入交换机124识别为下一跳，并且可以使L3联网设备118B和接入交换机124更新其ARP表、NDP邻居表、或其他IP-MAC地址映射信息。用于使联网设备更新L3-L2网络地址映射信息的许多其他方案也是可能的，并且本领域的普通技术人员可以设想这些情况并理解它们在本公开的范围内。

[0050] 网络管理系统110可以通过诸如经由网络管理云(例如，网络管理云102)中的L3联网设备(例如，L3联网设备118A)向L3联网设备118B发送请求306以取得信息以更新L3-L2网络地址映射信息，来开始确定端点128的唯一身份。在一些实施例中，网络管理系统110可以以规则的时间间隔发送请求306，这可以由管理员经由用户接口(例如，用户接口层234)来配置。替代地或附加地，请求306可以由事件触发，诸如联网设备或端点由于网络故障而断开连接然后重新连接至网络管理系统110、联网设备或端点首次或自设备上次连接到网络管理系统110以来预定时间段(也可是可配置的)之后连接至网络管理系统110、L3网络地址的手动分配、或DHCP服务器的重启或重新配置、等等。

[0051] 如所讨论的，网络管理系统110可以直接或间接地利用任何数量的协议或技术来从网络中的联网设备和端点取得L3-L2网络地址映射信息。为了简单和简洁，在该示例中，网络管理系统110可以利用SNMP来从L3联网设备118B请求ARP表信息。在其他实施例中，网络管理系统110可以从其他发现协议或技术接收CDP、LLDP、ISDP或NDP邻居设备信息或类似信息；使用DHCP、SNMP、ICMP、ARP、NDP或类似的网络管理协议和技术来探测设备信息；或使用API(例如NETCONF/YANG、gRPC、或OpenFlow™、或诸如SSH或Telnet的应用、以及本领域普通技术人员已知的其他示例)以编程方式获取设备信息。

[0052] 响应于SNMP请求306，L3联网设备118B可以向网络管理系统110发送SNMP响应308，该SNMP响应308可以包括接入交换机124的IP-MAC网络地址映射。在一些实施例中，L3联网设备118B可以将SNMP响应308中的映射限制为属于私有云104的IP网络地址。替代地或另外，L3联网设备118B可以将SNMP响应308限制为增量信息(例如，新的或更新的端点身份)。

[0053] 在从L3联网设备118B接收到L3-L2网络地址映射信息之后，网络管理系统110可以分析L2网络地址以确定它们中的任一个是否对应于已知联网设备，例如通过参考设备数据库(例如，设备数据库240)、联网设备数据库(例如，联网设备数据库242)、端点数据库(例如，端点数据库244)、或类似信息。在此示例中，IP-MAC地址映射信息(例如，L3联网设备的ARP表或ARP表的一部分)可以包括端点128的IP地址到接入交换机124的MAC地址的映射，接入交换机124可以是私有云104中的已知联网设备。过程300可以继续进行，网络管理系统110将SNMP请求310发送到接入交换机124，以获取其IP-MAC地址映射信息(例如，接入交换机的ARP表或ARP表的一部分)。接入交换机124可以发送包括所请求的信息的SNMP响应312。

[0054] 网络管理系统110随后可以解析SNMP响应312中的IP-MAC地址映射信息中的MAC地址，以确定它们中的任一个是否对应于已知联网设备。在该示例中，从接入交换机124接收的IP-MAC地址映射可以将端点128的IP地址与接入点126的MAC地址相关联，接入点126可以是私有云104中的已知联网设备。结果，网络管理系统110可以将SNMP请求314发送到接入点126以获取其IP-MAC地址映射(例如，接入点的ARP表或ARP表的一部分)。接入点126可以发送包括这些映射的SNMP响应316。

[0055] 更新过程300可以以网络管理系统110检查SNMP响应316中的IP-MAC地址映射以评

估是否有任何MAC地址对应于已知联网设备来结束。在该示例中，从接入点126接收的IP-MAC地址映射可以将端点128的IP地址与其真实的MAC地址进行映射。因此，网络管理系统110可以使用针对端点128的真实IP-MAC地址映射来更新设备数据库240(和/或端点数据库244)。

[0056] 图3B示出了用于更新L3-L2网络地址的映射以唯一地识别跨L3网络的端点的集中管理和分布式过程320的流程图的示例。过程320在某些方面可以类似于过程300，例如包括802.11关联322和DHCP、ARP、或NDP表、或类似的IP-MAC地址映射信息的更新324。然而，在该示例中，代替如过程300中那样网络管理系统110直接取得L3-L2网络地址映射信息，过程320示出了一个或多个上游网络或设备(例如，L3联网设备118B和接入交换机124)可以将对映射信息的请求(例如，分别为SNMP请求328和330)传播到下游设备(例如，分别为接入交换机124和接入点126)，在下游设备上等待，以及然后发送响应(例如，分别为SNMP响应332和334)。过程320可以以L3联网设备118B向网络管理系统110发送响应(例如，SNMP响应336)结束。

[0057] 图3C示出了用于识别跨L3网络的端点的唯一身份的分散和本地控制的过程340的流程图的示例。在该示例中，代替过程300中的集中式控制器(例如，网络管理系统110)启动识别过程并从联网设备拉取L3-L2网络地址映射信息，网络的一个或多个下游联网设备(例如，接入点126、接入交换机124、L3联网设备118B、安全设备116B等)能够将映射信息推送到上游联网设备。

[0058] 在此示例中，过程340可以从802.11关联342开始，并更新344DHCP、ARP或NDP邻居表、或类似的IP-MAC地址映射信息。这些更新可以触发识别过程，该过程始于接入点126向接入交换机124发送SNMP消息346(或其他合适协议的消息)，该消息可包括通告端点128的IP地址到端点的真实MAC地址的映射的信息。继而，接入交换机124可以发送SNMP确认(ACK)348。然后，接入点126可以向L3联网设备118B发送类似的SNMP消息350，该消息可以包括端点128的IP地址和端点的真实MAC地址的映射的通告。L3联网设备118B可以发送SNMP ACK352。在一些实施例中，接入点126可以同时发送SNMP消息346和350。

[0059] 在一些实施例中，每个能够发起端点识别过程的联网设备都可以维护本地L3-L2网络地址映射数据库，以唯一地识别网络的端点。这样的联网设备可以分析流经它的流量，将流量的L3和L2网络地址与本地L3-L2网络地址映射数据库进行比较，并在检测到新的或更新的L3-L2网络地址映射后向一个或更多上游联网设备发送新的或更新的映射的通告。

[0060] 图3D示出了用于识别跨L3网络的端点的唯一身份的分散和分布式过程360的流程图的示例。过程360可以以802.11关联362开始，并更新364DHCP、ARP、或NDP表、或类似的IP-MAC地址映射信息。然而，代替如过程340中那样接入点126控制整个端点识别过程，接入交换机124可以响应于从接入点126接收到SNMP通告368而向L3联网设备118B发送SNMP通告370。过程360可以以L3联网设备118B响应于SNMP通告460向接入交换机124发送SNMP ACK 372而结束。

[0061] 在一些实施例中，网络可以执行集中式更新过程300和320以及分散过程340和360的不同排列。例如，在实施例中，端点128可以通过向网络管理系统发送端点的IP地址和端点的真实MAC地址的新的或更新的映射的通告，来发起更新过程，并且网络管理系统110之后可以类似于过程300来控制更新过程，或者使SNMP消息分发到网络的其他联网设备，类似

于过程320。在另一个实施例中，私有云104中的联网设备(例如，安全设备116B、L3联网设备118B等)可以集中管理更新过程，而无需外部网络管理系统。在又一个实施例中，私有云104中的独立服务器(例如，物理或虚拟)可以管理更新过程。本领域普通技术人员将理解，在不脱离本公开的范围的情况下，还可以实现其他排列。

[0062] 图4示出了用于管理跨L3网络的端点的唯一身份的过程400的示例。如所讨论的，过程400可以由第一L3网络(例如，网络管理云102)中的集中式网络控制器(例如，网络管理系统110)来管理，或者可以由第二L3网络(例如，私有云104)中的联网设备(例如，安全设备116B、L3联网设备118B、接入交换机124、接入点126等)来分散和管理，其中，联网设备本身可以作为网络管理系统操作。

[0063] 在此示例中，过程400可以从步骤402开始，在该步骤中，网络管理系统以及特别是第一L3网络(网络管理云102，或者在一些情况下，私有云104的第一L3网络段)中的网络管理系统的第一L3联网设备(例如，L3联网设备118A、安全设备116B、L3联网设备118B、接入交换机126、接入点126等)可以从第二L3网络(例如，私有云104，或者在一些情况下，私有云104的第二L3网络段)中的第二L3联网设备接收L3-L2网络地址映射信息。在一些实施例中，可以响应于网络管理系统的第一L3联网设备的请求来接收映射信息。例如，第一L3联网设备可以将SNMP请求发送到第二L3联网设备，以获取第二设备的ARP表、NDP邻居表、或其他IP-MAC网络地址映射信息。在一些实施例中，第一L3网络和第二L3网络可以是分开的网络。例如，第一L3网络可以是云提供商网络，并且第二L3网络可以是云提供商的客户的私有网络。在其他实施例中，第一和第二L3网络可以包括同一私有网络(例如主校园网络和分支机构网络、第一地理区域(例如，美国、美国西海岸、北加利福尼亚等)中的数据中心和第二地理区域(例如，欧洲、美国东海岸、南加利福尼亚等)中的数据中心、会计部门网络和人力资源部门网络等)的L3网络段。

[0064] 在步骤404中，网络管理系统可以分析L3-L2网络地址映射信息，以确定L2网络地址是否与第二L3网络中的另一个联网设备(例如，第三联网设备)相关联。例如，网络管理系统可以使用映射信息中的MAC地址作为查询的关键词或索引来查询设备数据库(例如，设备数据库24)、联网设备数据库(例如，联网设备数据库242)、端点数据库(例如，端点数据库244)、和/或类似数据源。

[0065] 在判定框406处，如果第一L2网络地址与联网设备相关联，则过程400可以返回至步骤402，以确定下游设备(例如，第三L3联网设备)的第一L3-L2网络地址映射信息是否将第一L3网络地址映射到联网设备。步骤402和404以及判定块406可以重复任意次数，直到下游设备的L3-L2网络地址映射信息将第一L3网络地址映射到端点为止。在一些实施例中，网络管理系统可以使用下游联网设备的L3网络地址作为端点的标识符，直到网络管理系统可以识别端点的真实L2网络地址，以避免对需要端点的标识符的其他网络操作的阻止。

[0066] 在判定框406处，如果相反网络管理系统评估的当前L2网络地址与端点相关联，则过程400可以前进至步骤408。在步骤408处，网络管理系统可以将第一L3网络地址和当前L2网络地址存储作为第二L3网络中的端点的唯一身份。

[0067] 过程400可以继续至步骤410，其中网络管理系统可以监视去往和来自第二L3网络中的L3网络地址的网络流量，以及步骤412，其中网络管理系统可以基于端点的唯一身份将流量与端点相关联。以这种方式，网络管理系统可以指定跨L3网络的端点的网络利用。例

如,网络管理系统可能与端点不在同一个广播域中,但是网络管理系统仍然可以能够基于端点的唯一身份从其L3网络地址解析端点的L2网络地址。

[0068] 以这种方式,即使当端点可以在一段时间内的不同时间共享相同的L3网络地址时,网络管理系统也可以区分不同的端点进行的网络活动。例如,可以在一天的第一部分为第一端点分配IP地址,并且可以在一天的稍后部分为第二端点分配同一IP地址。但是,网络管理系统可以正确地将在一天的第一部分期间发生到IP地址的网络活动归因于第一端点,并将在一天的稍后部分期间发生到IP地址的网络活动归因于第二端点。

[0069] 过程400可以在步骤414结束,在该步骤中,网络管理系统可以基于端点唯一身份使用与端点相关的网络流量来呈现端点的网络利用信息。

[0070] 图5示出了用于使用与跨L3网络的端点的唯一身份相关的流量来呈现该端点的网络利用信息的用户界面500的示例。用户界面500只是用于呈现端点的状态信息的用户界面的一个示例。其他实施例可以包括更少数量或更多数量的元素。在该示例中,用户界面500可以包括端点信息窗格502、定位窗格504、网络利用窗格506、网络策略窗格510、网络信息窗格512和网络连接性窗格514。

[0071] 端点信息窗格502可以显示有关端点的各种有用信息,例如其主机名或设备名称、相对于网络管理系统的连接状态、SSID、接入点、射频(RF)信号强度、RF信道、用户、类型、制造商、型号、功能和其他元数据。定位窗格504可以显示端点的地理位置。网络利用窗格506可以包括一段时间(例如,小时、天、周、月、等)内带宽使用(例如,Mb/s、Gb/s等)的摘要视图(例如,x-y图)。网络利用窗格506还可以包括在同样的时间段内下载和上传的字节总数。另外,网络利用窗格506可以使用户能够选择端点的网络活动的更精细的视图,例如端点的帧、分组、流、连接、会话、或其他网络数据的各种粒度级别的视图。在一些实施例中,网络利用窗格506可以显示在端点上运行的应用的网络利用的摘要视图508(例如,饼图)。

[0072] 网络策略窗格510可以显示与端点相关联的网络策略,例如带宽限制、L3防火墙规则的数量、层7防火墙规则的数量、流量整形规则的数量等等。网络信息窗格512可以显示关于端点的网络相关信息,例如其IPv4地址、IPv6地址、MAC地址、VLAN等等。网络连接性窗格514可以显示端点的网络连接的当前状态,例如网络时延量、分组丢失率、平均时延等等。

[0073] 图6示出了联网设备600(例如,安全设备116、L3联网设备118、接入交换机124、接入点126等)的示例。联网设备600可以包括主中央处理单元(CPU)602、接口604和总线606(例如,PCI总线)。当在适当的软件或固件的控制下动作时,CPU 602可以负责执行分组管理、错误检测、和/或路由功能。CPU 602优选地在包括操作系统和任何适当的应用软件的软件的控制下完成所有这些功能。CPU 602可以包括一个或多个处理器608,诸如来自摩托罗拉微处理器家族或MIPS微处理器家族的处理器。在替代实施例中,处理器608可以是用于控制联网设备600的操作的专门设计的硬件。在实施例中,存储器610(诸如非易失性RAM和/或ROM)也可以形成CPU 602的一部分。但是,存在可以将存储器耦合到系统的多种不同的方式。

[0074] 接口604可以被提供为接口卡(有时被称为线卡)。接口604可以控制通过网络的数据分组的发送和接收,并且有时支持与联网设备600一起使用的其他外围设备。可以提供的接口包括以太网接口、帧中继接口、电缆接口、DSL接口、令牌环接口等。另外,可以提供各种非常高速的接口,例如快速令牌环接口、无线接口、以太网接口、千兆位以太网接口、异步传

输模式(ATM)接口、高速串行接口(HSSI)、SONET上分组(POS)接口、光纤分布式数据接口(FDDI)等。接口604可以包括适合于与适当的介质进行通信的端口。在一些情况下,接口604还可以包括独立处理器,并且在一些情况下还包括易失性RAM。独立处理器可以控制通信密集型任务,例如分组交换、介质控制和管理。通过为通信密集型任务提供单独的处理器,接口604可以允许CPU 602有效地执行路由计算、网络诊断、安全功能等等。

[0075] 尽管图6所示的系统是实施例的联网设备的示例,但它绝不是可以在其上实现主题技术的唯一联网设备架构。例如,也可以使用具有可处理通信以及路由计算和其他网络功能的单个处理器的架构。此外,其他类型的接口和介质也可以与联网设备600一起使用。

[0076] 不管联网设备的配置如何,它都可以采用一个或多个存储器或存储器模块(包括存储器610),该存储器或存储器模块被配置为存储用于通用网络操作的程序指令以及用于本文描述的漫游、路由优化和路由功能的机制。程序指令可以控制操作系统和/或一个或多个应用的操作。一个或多个存储器还可以被配置为存储诸如移动性绑定、注册和关联表等的表。

[0077] 图7A和图7B示出了根据各种实施例的系统。在实践各种实施例时,更合适的系统对于本领域普通技术人员将是显而易见的。本领域普通技术人员也将容易理解,其他系统是可能的。

[0078] 图7A示出了总线计算系统700的示例,其中系统的组件使用总线705彼此电通信。计算系统700可以包括处理单元(CPU或处理器)710和系统总线705,该系统总线705可以将包括诸如只读存储器(ROM)720和随机存取存储器(RAM)725之类的系统存储器715的各种系统组件耦合至处理器710。计算系统700可以包括与处理器710直接连接、紧密接近或集成为其一部分的高速存储器的高速缓存712。计算系统700可以将数据从存储器715、ROM 720、RAM 725、和/或存储设备730复制到高速缓存712以供处理器710快速访问。以这种方式,高速缓存712可以提供性能提升,从而避免了处理器在等待数据时的延迟。这些模块和其他模块可以控制处理器710执行各种动作。其他系统存储器715也可供使用。存储器715可以包括具有不同性能特性的多种不同类型的存储器。处理器710可以包括任何通用处理器和硬件模块或软件模块,例如存储在存储设备730中的模块1 732、模块2 734和模块3 736,其被配置为控制处理器710,以及包括专用处理器,其中软件指令被并入实际的处理器设计。处理器710可以实质上是完全自包含的计算系统,包含多个核或处理器、总线、存储器控制器、高速缓存等。多核处理器可以是对称的或非对称的。

[0079] 为了使用户能够与计算设备700进行交互,输入设备745可以表示任意数量的输入机制,例如用于语音的麦克风、用于手势或图形输入的触摸保护屏幕、键盘、鼠标、运动输入、语音等等。输出设备735也可以是本领域技术人员已知的许多输出机制中的一个或多个。在一些情况下,多模态系统可以使用户能够提供多种类型的输入以与计算设备700通信。通信接口740可以支配和管理用户输入和系统输出。对于在任何特定硬件装置上的操作可以没有限制,因此在开发它们时,此处的基本功能可以很容易地替换为改进的硬件或固件装置。

[0080] 存储设备730可以是非易失性存储器,并且可以是硬盘或可以存储可由计算机访问的数据的其他类型的计算机可读介质,例如磁带、闪存卡、固态存储设备、数字通用盘、盒式磁带、随机存取存储器、只读存储器、及其混合。

[0081] 如以上讨论的，存储设备730可以包括用于控制处理器710的软件模块732、734、736。可以构想其他硬件或软件模块。存储设备730可以连接到系统总线705。在一些实施例中，执行特定功能的硬件模块可以包括与必要的硬件组件(例如，处理器710、总线705、输出设备735等)相关联地存储在计算机可读介质中的软件组件以执行该功能。

[0082] 图7B示出了根据实施例可以使用的芯片组计算系统750的示例架构。计算系统750可以包括处理器755，其代表能够执行被配置为执行所识别的计算的软件、固件和硬件的任何数量的物理和/或逻辑上不同的资源。处理器755可以与芯片组760通信，该芯片组760可以控制到处理器755的输入和从处理器755的输出。在该示例中，芯片组760可以将信息输出到诸如显示器的输出设备765，并且可以读取和写入信息到存储设备770，存储设备770可以包括磁性介质、固态介质和其他合适的存储介质。芯片组760还可以从RAM 775读取数据并将数据写入RAM 775。可以提供用于与各种用户接口组件785接口的桥接器780，用于与芯片组760接口。用户接口组件785可以包括键盘、麦克风、触摸检测和处理电路、点选设备(例如鼠标)等。对计算系统750的输入可以来自机器生成和/或人工生成的多种来源中的任一种。

[0083] 芯片组760还可以与可具有不同物理接口的一个或多个通信接口790接口。通信接口790可以包括用于有线和无线LAN、用于宽带无线网络、以及个域网的接口。用于生成、显示和使用本文公开的技术的方法的一些应用可以包括通过物理接口接收排序的数据集，或者由机器本身通过处理器755分析存储在存储设备770或RAM 775中的数据来生成。另外，计算系统750可以经由用户接口组件785接收来自用户的输入，并通过使用处理器755解释这些输入来执行适当的功能，例如浏览功能。

[0084] 将理解，计算系统700和750可以分别具有不止一个处理器710和755，或者可以是联网在一起以提供更大处理能力的计算设备组或群集的一部分。

[0085] 为了解释清楚起见，在一些情况下，各种实施例可以被表示为包括各个功能块，这些功能块包括含设备、设备组件、以软件或硬件和软件的组合体现的方法中的步骤或例程的功能块。

[0086] 在一些实施例中，计算机可读存储设备、介质和存储器可以包括包含比特流等的电缆或无线信号。然而，当提及时，非暂态计算机可读存储介质明确地排除诸如能量、载波信号、电磁波和信号本身之类的介质。

[0087] 可以使用存储或以其他方式从计算机可读介质可用的计算机可执行指令来实现根据上述示例的方法。这样的指令可以包括例如引起或以其他方式配置通用计算机、专用计算机或专用处理设备以执行特定功能或功能组的指令和数据。可以通过网络访问使用的计算机资源的一部分。计算机可执行指令可以是例如二进制、中间格式指令，例如汇编语言、固件或源代码。可用于存储指令、所用信息、和/或在根据所述示例的方法期间创建的信息的计算机可读介质的示例包括磁盘或光盘、闪存、配备有非易失性存储器的通用串行总线(USB)设备、网络存储设备、等等。.

[0088] 实现根据这些公开的方法的设备可以包括硬件、固件和/或软件，并且可以采用多种外形中的任何一种。这样的外形的一些示例包括膝上型计算机、智能电话、小型外形的个人计算机、个人数字助理、机架安装设备、独立设备等等。本文描述的功能也可以体现在外围设备或附加卡中。作为进一步的示例，这种功能还可以在单个设备中执行的不同芯片或不同过程之间的电路板上实现。

[0089] 指令、用于传达这样的指令的介质、用于执行它们的计算资源、以及用于支持这样的计算资源的其他结构是用于提供这些公开中所描述的功能的手段。

[0090] 尽管使用各种示例和其他信息来解释所附权利要求的范围内的各方面，但是基于这样的示例中的特定特征或布置，不应该暗示对权利要求的限制，因为本领域普通技术人员将能够使用这些示例来推导各种各样的实现。此外，尽管可能已经以特定于结构特征和/或方法步骤的示例的语言描述了一些主题，但是应当理解，所附权利要求中定义的主题不必限于这些描述的特征或动作。例如，这种功能可以不同地分布在除本文所标识的组件之外的组件中或在其中执行。而是，所描述的特征和步骤被公开为在所附权利要求的范围内的系统和方法的组件的示例。

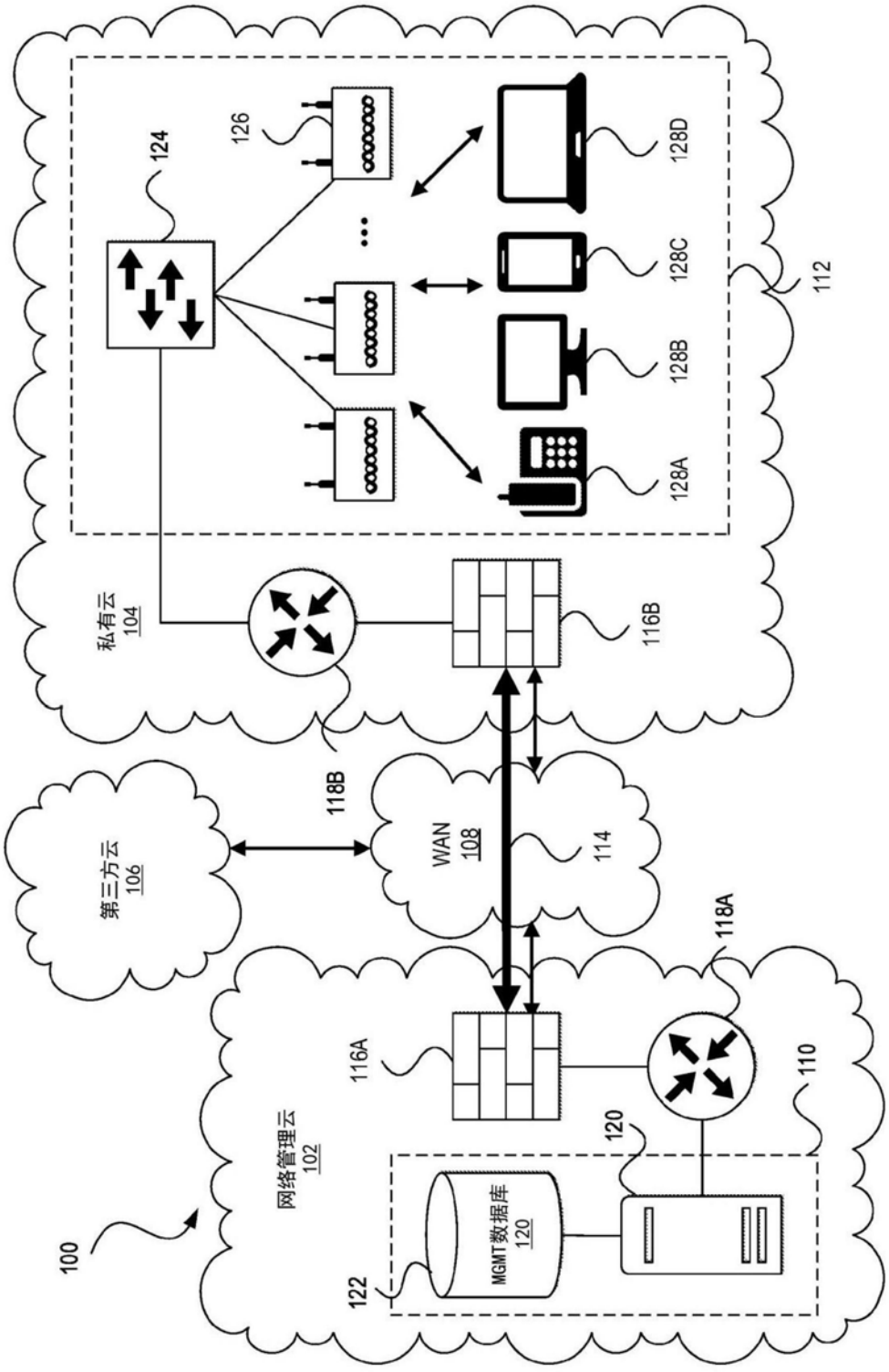

100
网络管理云
102
MGMT数据库
120
122
120
110
116A
118A
WAN
108
114
118B
第三方云
106
私有云
104
116B
112
124
126
128A
128B
128C
128D

图1

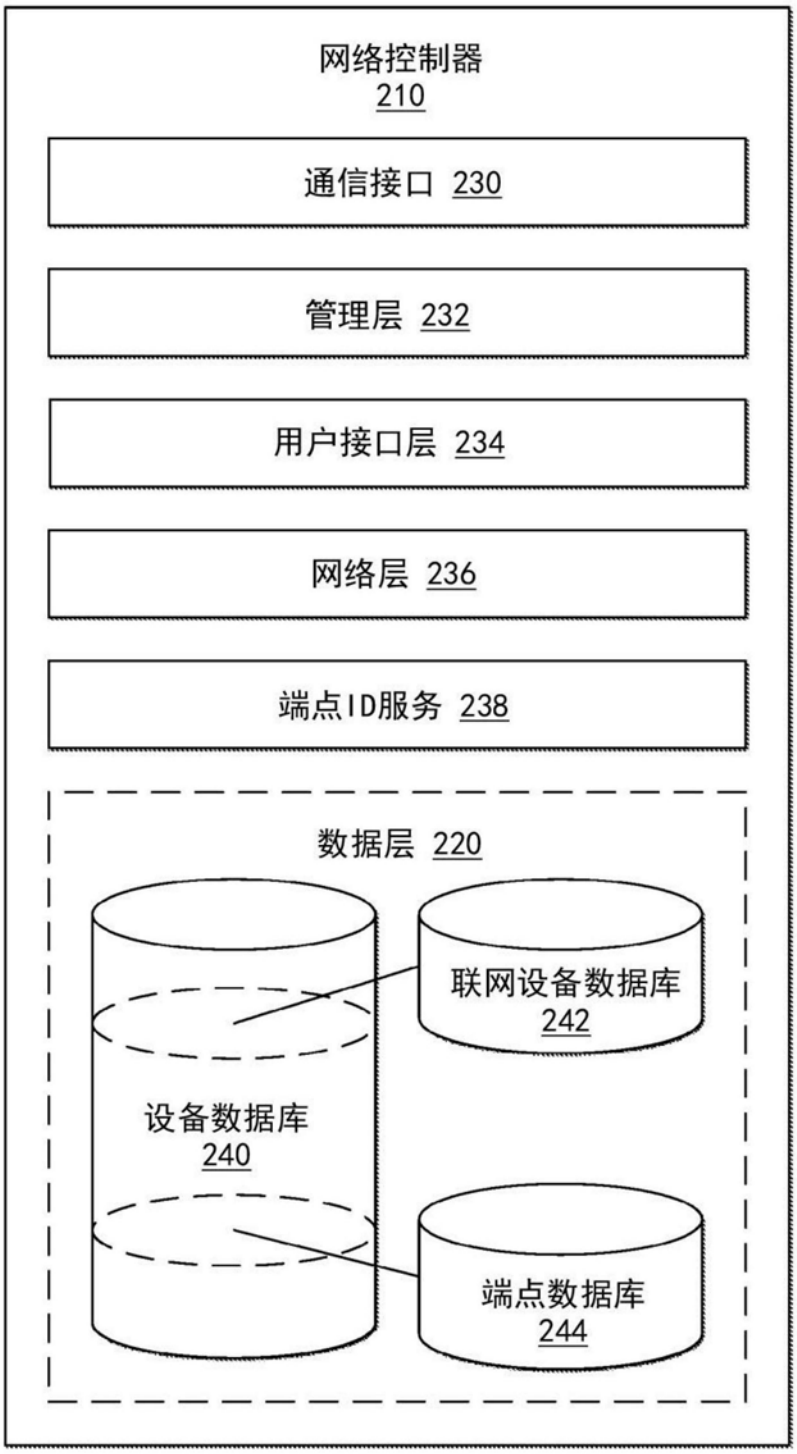

网络控制器
210
通信接口 230
管理层 232
用户接口层 234
网络层 236
端点ID服务 238
数据层 220
联网设备数据库
242
设备数据库
240
端点数据库
244

图2

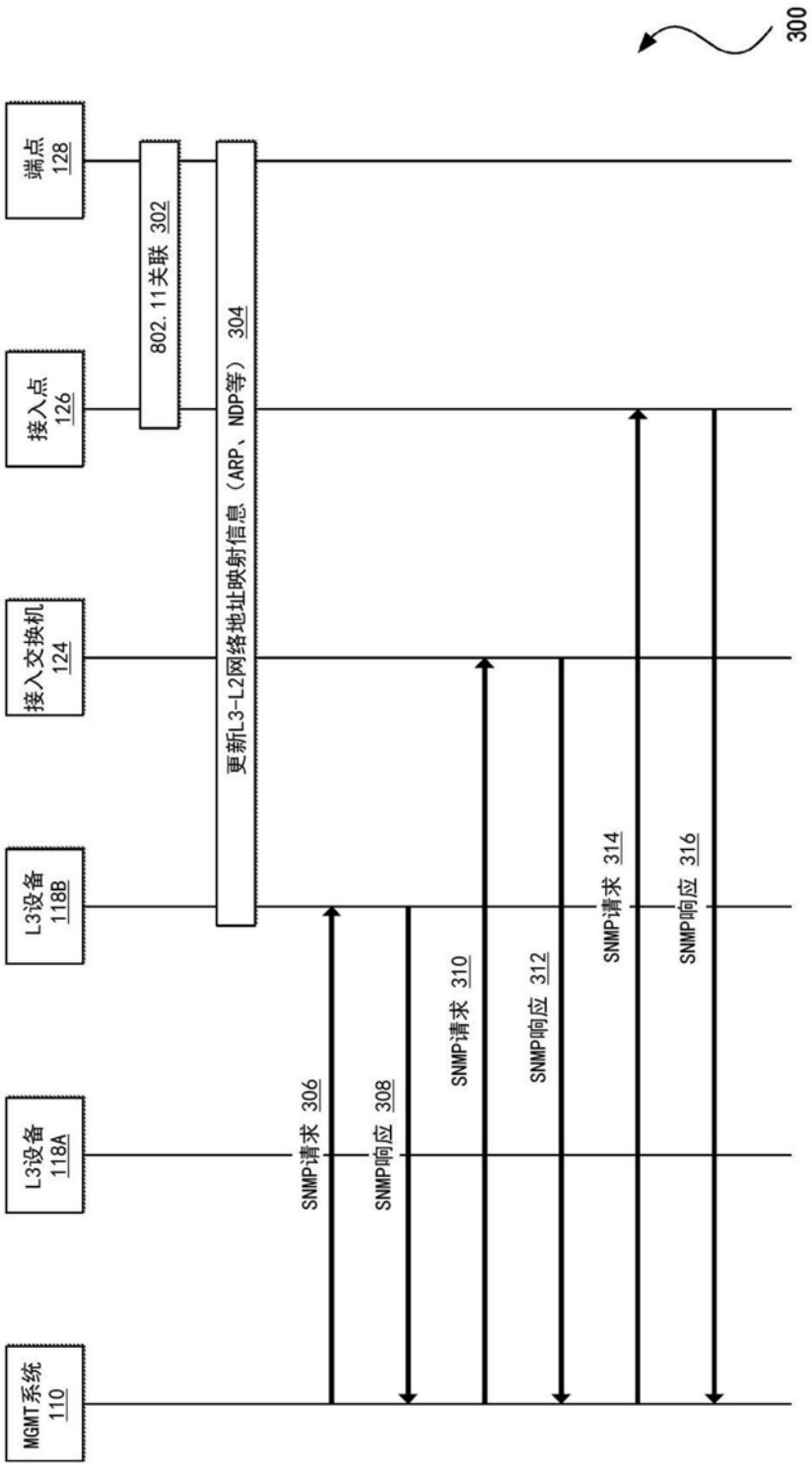

300
端点 128
802.11关联 302
接入点 126
更新L3-L2网络地址映射信息（ARP、NDP等） 304
接入交换机 124
L3设备 118B
SNMP请求 306
SNMP响应 308
SNMP请求 310
SNMP响应 312
SNMP请求 314
SNMP响应 316
L3设备 118A
MGMT系统 110

图3A

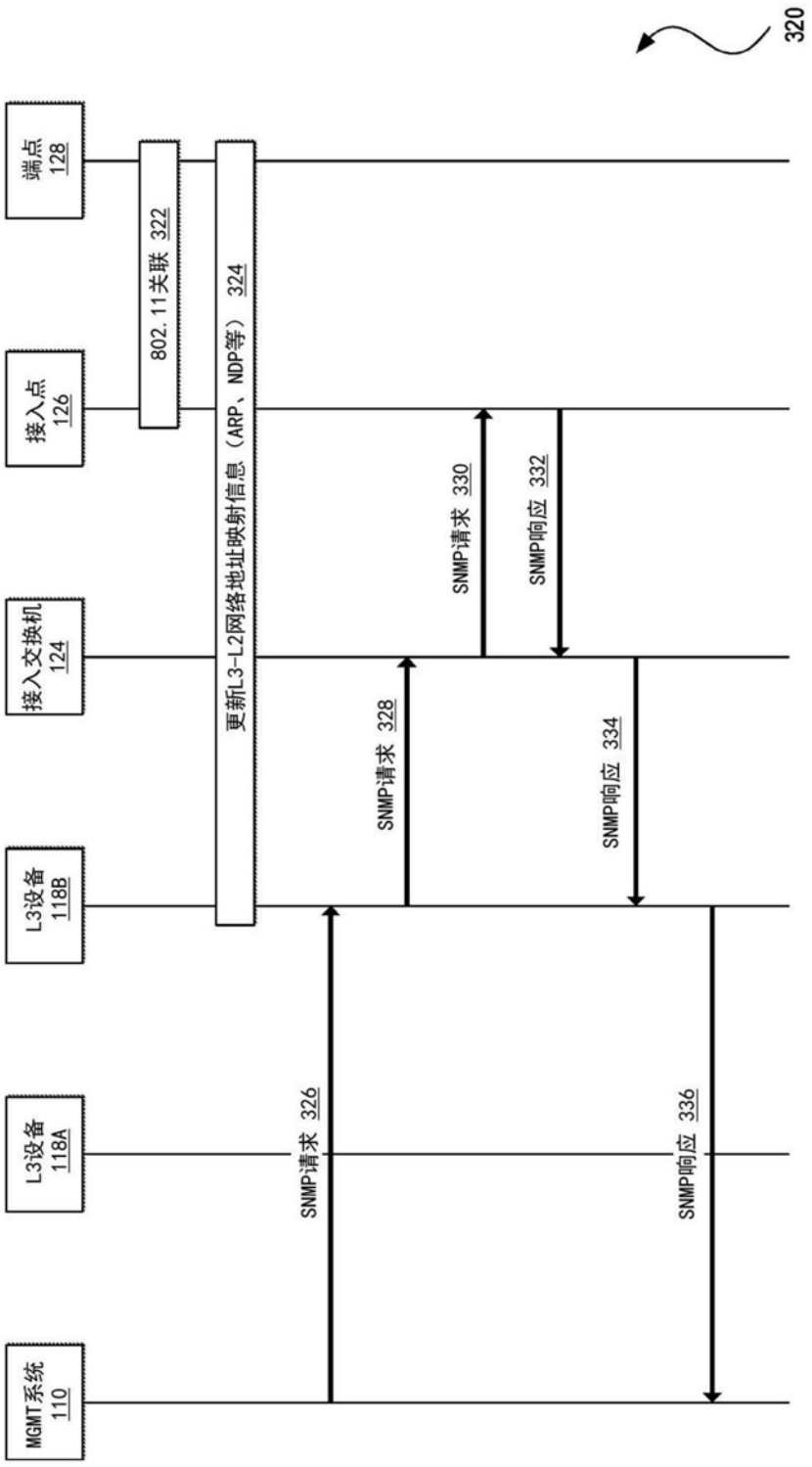

320
端点 128
接入点 126
接入交换机 124
L3设备 118B
L3设备 118A
MGMT系统 110
802.11关联 322
更新L3-L2网络地址映射信息（ARP、NDP等） 324
SNMP请求 330
SNMP响应 332
SNMP请求 328
SNMP响应 334
SNMP请求 326
SNMP响应 336

图3B

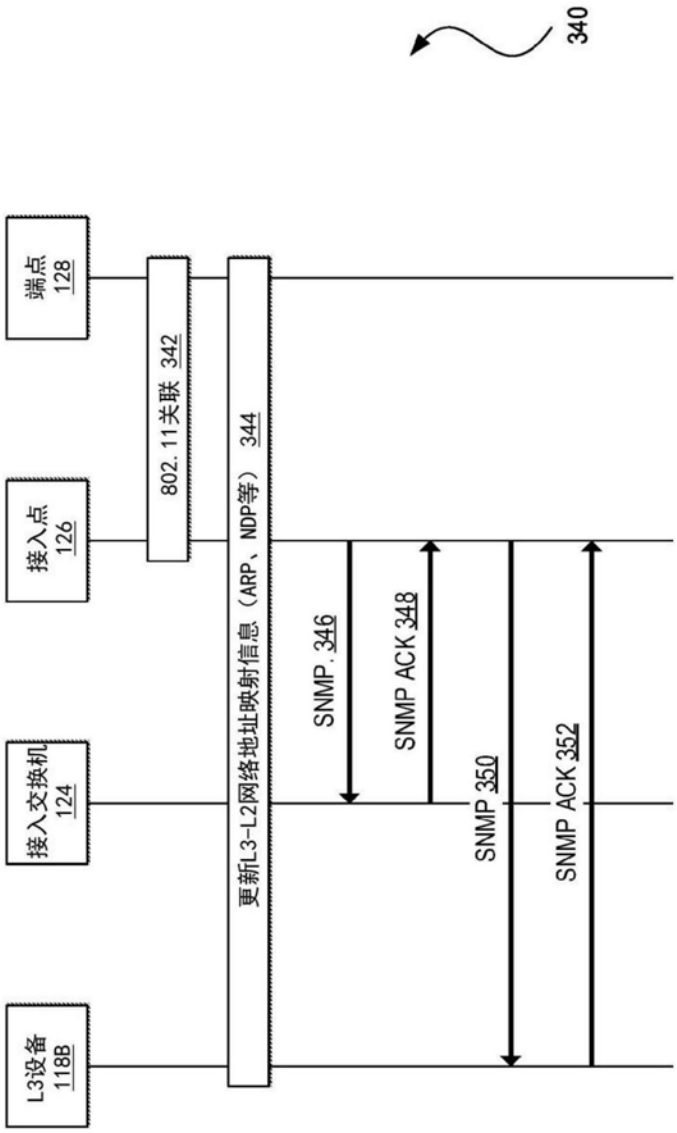

340
端点 128
接入点 126
接入交换机 124
L3设备 118B
802.11关联 342
更新L3-L2网络地址映射信息（ARP、NDP等） 344
SNMP 346
SNMP ACK 348
SNMP 350
SNMP ACK 352

图3C

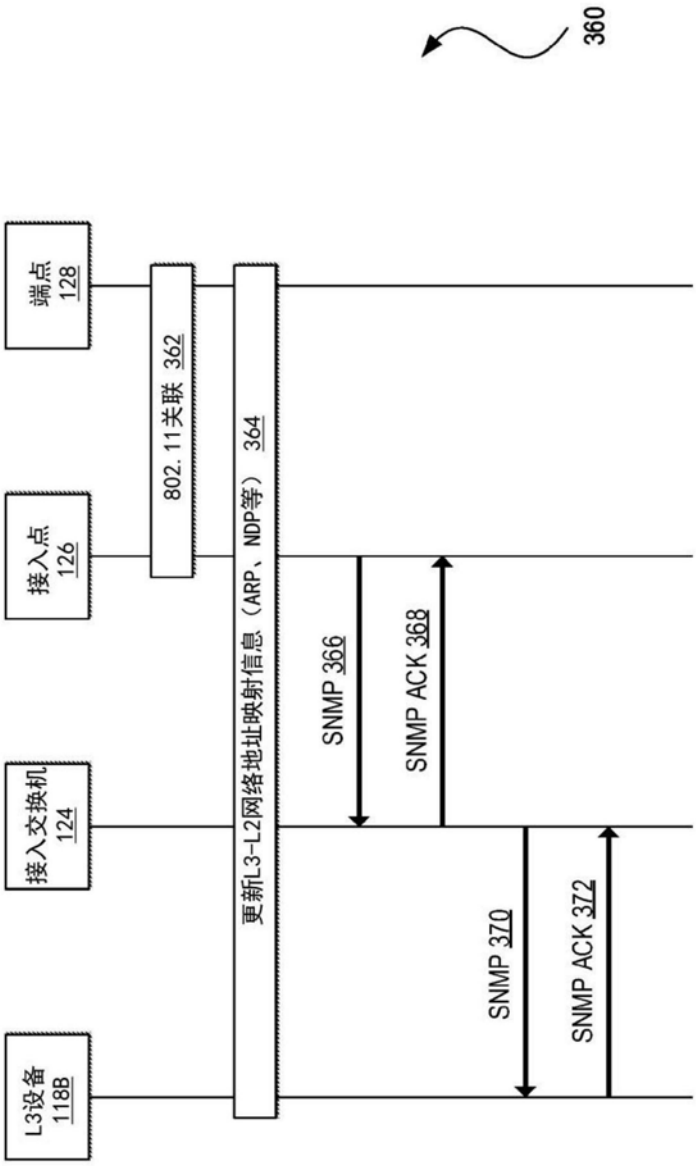

360
端点 128
接入点 126
接入交换机 124
L3设备 118B
802.11关联 362
更新L3-L2网络地址映射信息（ARP、NDP等） 364
SNMP 366
SNMP ACK 368
SNMP 370
SNMP ACK 372

图3D

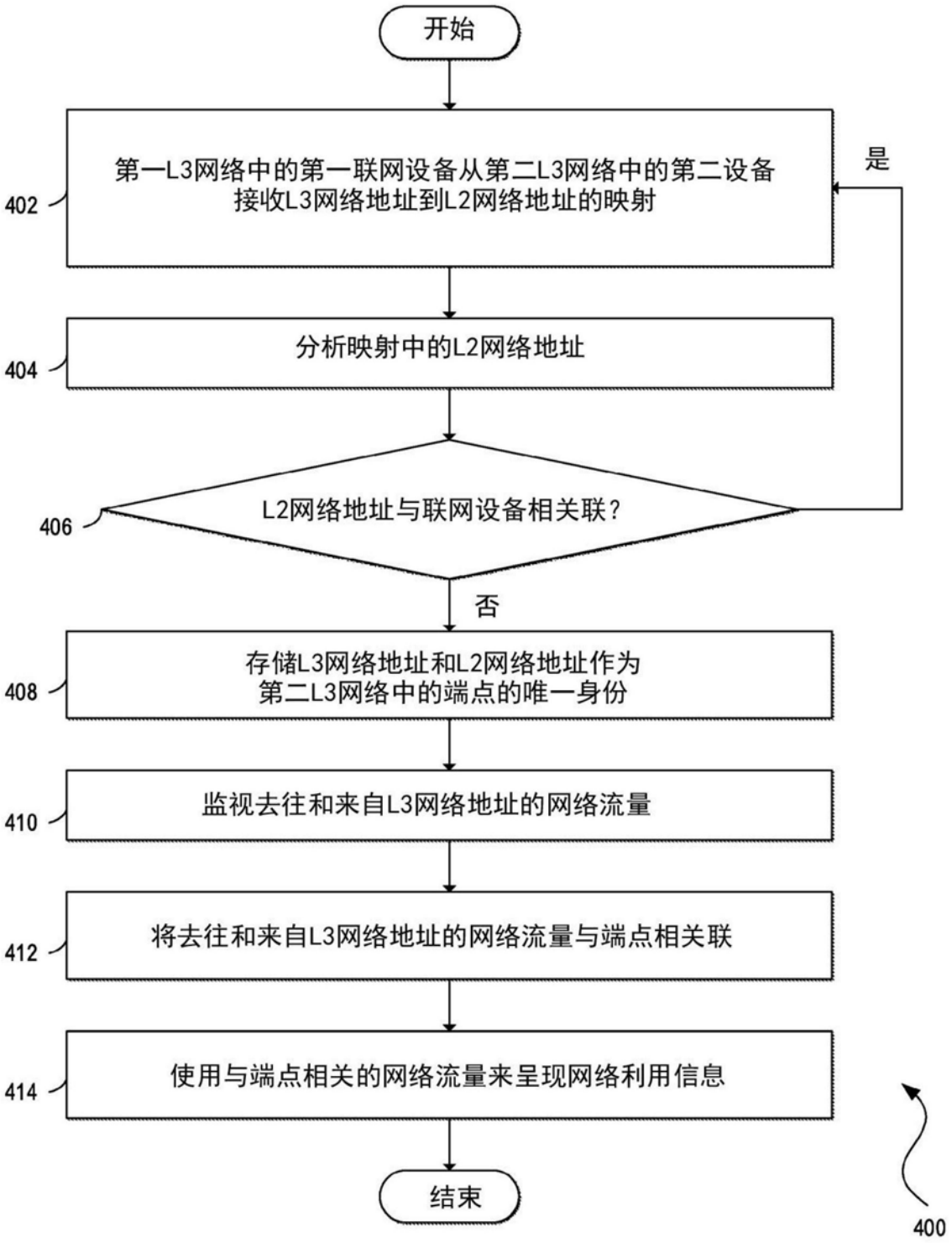

开始
第一L3网络中的第一联网设备从第二L3网络中的第二设备
接收L3网络地址到L2网络地址的映射
402
分析映射中的L2网络地址
404
L2网络地址与联网设备相关联？
406
是
否
存储L3网络地址和L2网络地址作为
第二L3网络中的端点的唯一身份
408
监视去往和来自L3网络地址的网络流量
410
将去往和来自L3网络地址的网络流量与端点相关联
412
使用与端点相关的网络流量来呈现网络利用信息
414
结束
400

图4

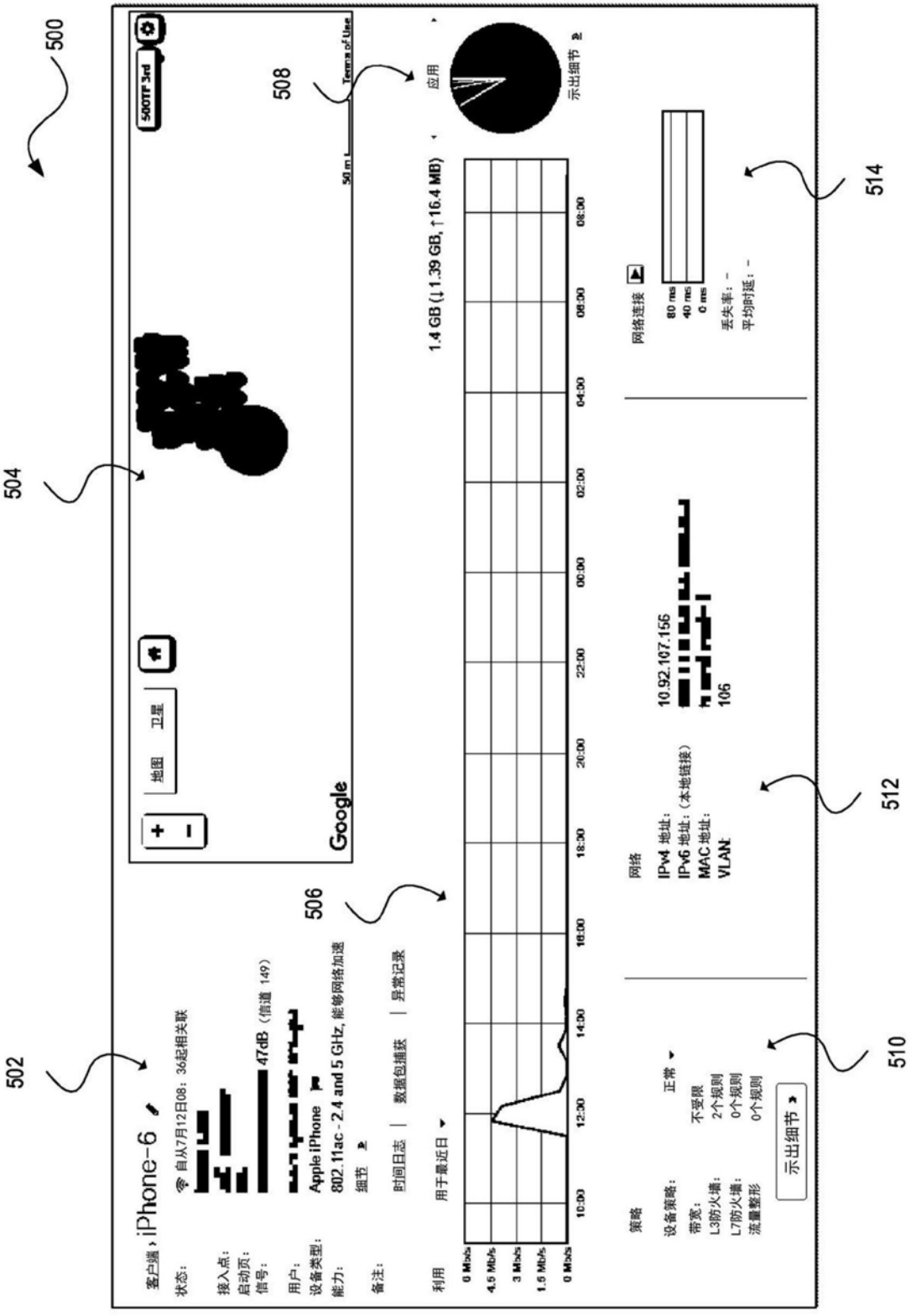

500
502
504
506
508
510
512
514
客户端，iPhone-6
状态：
接入点：
启动页：
信号：
用户：
设备类型：
能力：
备注：
Apple iPhone
802.11ac - 2.4 and 5 GHz, 能够网络加速
细节
时间日志 | 数据包捕获 | 异常记录
利用
用于最近日
策略
设备策略：
带宽：
L3防火墙：
L7防火墙：
流量整形
示出细节
网络
IPv4 地址：
IPv6 地址：（本地链接）
MAC地址：
VLAN
10.92.107.156
106
地图
卫星
Google
1.4 GB (↓1.39 GB, ↑16.4 MB)
应用
网络连接
丢失率：-
平均时延：-

图5

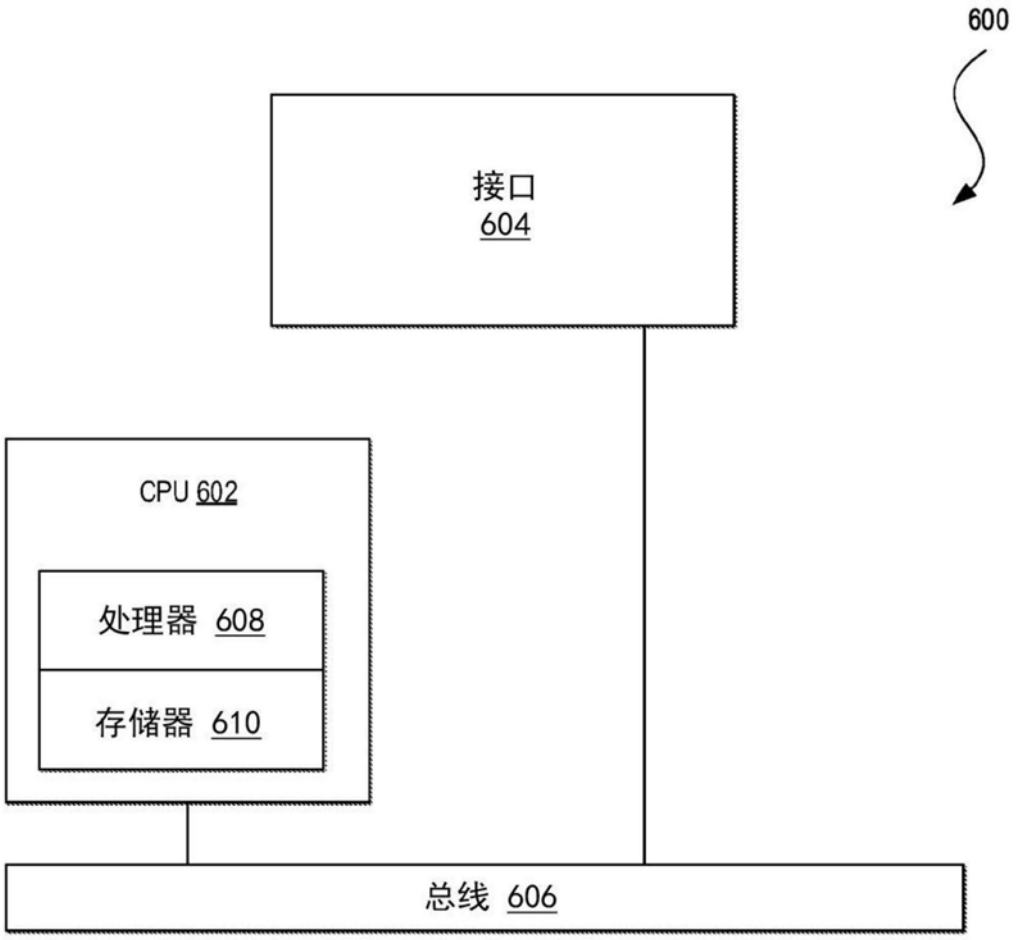

600
接口
604
CPU 602
处理器 608
存储器 610
总线 606

图6

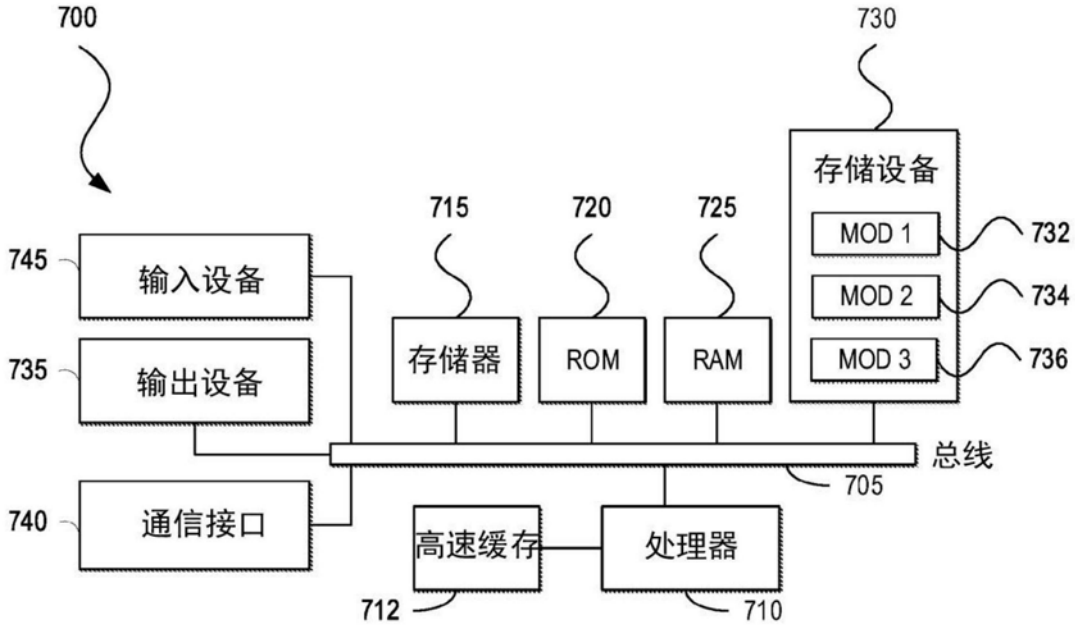

700
730
存储设备
MOD 1
MOD 2
MOD 3
732
734
736
715
720
725
745
输入设备
735
输出设备
存储器
ROM
RAM
总线
705
740
通信接口
高速缓存
处理器
712
710

图7A

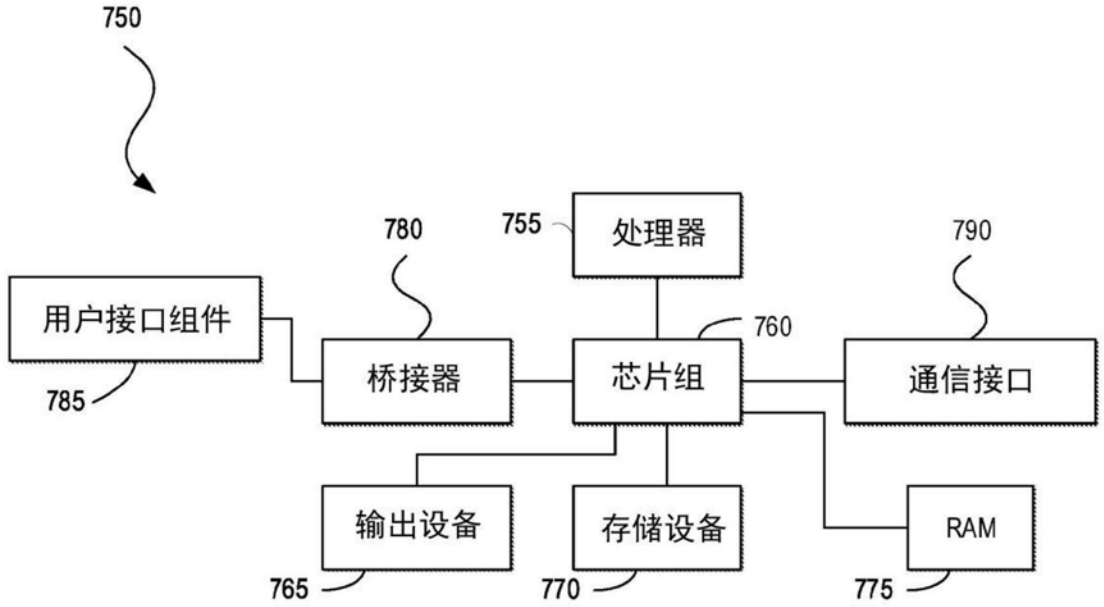

750
780
755
处理器
790
用户接口组件
760
桥接器
芯片组
通信接口
785
输出设备
存储设备
RAM
765
770
775

图7B