(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 113285864 A
(43)申请公布日 2021.08.20

(21)申请号 202110426315.2

(22)申请日 2016.01.28

(30)优先权数据
PCT/IB2016/00110 2016.01.05 IB
62/108,987 2015.01.28 US
62/144,293 2015.04.07 US
62/151,174 2015.04.22 US
62/174,394 2015.06.11 US
PCT/US2015/064242 2015.12.07 US
62/266,060 2015.12.11 US

(62)分案原申请数据
201680007187.5 2016.01.28

(71)申请人 安博科技有限公司
地址 中国香港皇后大道中340号华秦国际大厦20层2006室

(72)发明人 J·E·鲁本斯坦
J·A·D·克努森
T·A·B·J·圣马丁 C·E·奥尔
F·布鲁萨尔

(74)专利代理机构 北京允天律师事务所 11697
代理人 李建航 高源

(51)Int.Cl.
H04L 12/46(2006.01)
H04L 12/715(2013.01)
H04L 12/721(2013.01)
H04L 29/06(2006.01)
H04L 29/12(2006.01)

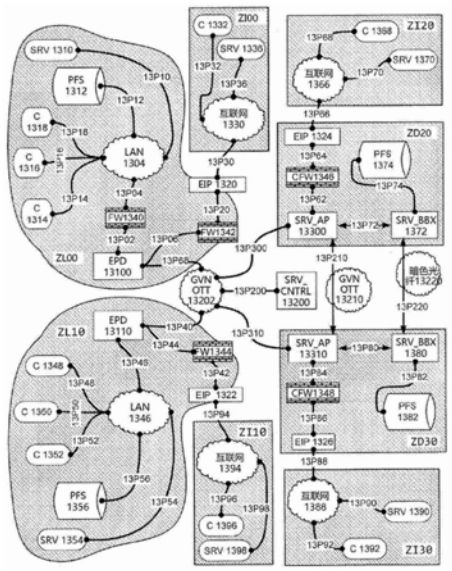
权利要求书1页 说明书49页 附图61页

(54)发明名称

用于全局虚拟网络的系统和方法

(57)摘要

本发明公开了用于经由虚拟全局网络来连接设备的系统和方法。在一个实施例中,所述网络系统可以包括与第一端点设备通信的第一设备以及与第二端点设备通信的第二设备。所述第一设备和所述第二设备可与通信路径连接。所述通信路径可以包括将每个端点设备连接至一个或多个中间接入点服务器和一个或多个控制服务器的一个或多个中间隧道。



CN 113285864 A

1.一种用于经由全局虚拟网络来连接设备的网络系统,包括:

与第一端点设备通信连接的第一设备;

与第二端点设备通信连接的第二设备;以及

连接所述第一端点设备和第二端点设备的通信路径,所述通信路径还包括一个或多个中间隧道,所述一个或多个中间隧道将每个端点设备连接到一个或多个中间接入点服务器以及一个或多个控制服务器。

2.根据权利要求1所述的网络系统,其中所述第一端点设备和所述中间接入点服务器中的至少一个被配置用于执行域名系统查找以便定位所述第二设备。

3.根据权利要求1所述的网络系统,其中所述第一端点设备和所述中间接入点服务器中的至少一个被配置用于从高速缓存中执行域名系统查找以便定位所述第二设备。

4.根据权利要求1所述的网络系统,其中所述中间接入点服务器中的至少一个被配置用于缓存内容。

5.根据权利要求1所述的网络系统,其中所述端点设备和所述中间接入点服务器中的至少一个被配置用于执行智能路由。

6.根据权利要求5所述的网络系统,其中所述智能路由基于最佳带宽、最低延迟时间、最少跳跃和无分组丢失中的至少一个。

7.根据权利要求5所述的网络系统,其中所述智能路由基于实时统计和历史统计中的至少一个。

8.根据权利要求1所述的网络系统,其中所述端点设备和所述中间接入点服务器中的至少一个被配置用于执行防火墙服务。

9.根据权利要求8所述的网络系统,其中所述第一端点设备在所述第一设备与所述中间接入点服务器之间提供防火墙服务。

10.根据权利要求8所述的网络系统,其中中间接入点服务器在第一端点设备与其他中间接入点服务器或所述第二端点设备之间提供防火墙服务。

用于全局虚拟网络的系统和方法

[0001] 本发明专利申请是申请日为2016年1月28日、申请号为 201680007187.5、发明名称为“用于全局虚拟网络的系统和方法”的发明专利申请的分案申请。

[0002] 本申请主张2015年1月28日提交的第62/108,987号美国临时专利申请、2015年4月7日提交的第62/144,293号美国临时专利中请、2015 年4月22日提交的第62/151,174号美国临时专利申请、2015年6月11 日提交的第62/174,394号美国临时专利申请、2015年12月7日提交的第PCT/US2015/064242号国际专利申请、2015年12月11日提交的第 62/266,060号美国临时专利申请以及2016年1月5日提交的第 PCT/US2016/012178号国际专利申请的优先权,这些申请均以引用方式并入本文中。2014年12月8日提交的第62/089,113号美国临时专利申请和2015年1月6日提交的第62/100,406号美国临时专利申请以引用方式并入本文中。

技术领域

[0003] 本公开总体上涉及网络,更具体地,涉及全局虚拟网络(GVN)的配置和操作。

背景技术

[0004] 尽管“最后一英里连接性”近年来已经极大地改善,但由于距离、协议限制、对等操作、干扰相关问题以及其他问题和威胁,仍然存在远距离连接性及吞吐量的问题。GVN在客户端标准互联网连接的顶部为客户端提供安全网络优化服务。

[0005] 本申请对GVN组成部分进行了概述并且对可用作GVN元素的相关技术进行了描述。GVN元素可独立地或在GVN生态系统中操作,诸如出于其自身目的采用GVN架构,或可被部署以增强GVN的性能和效率。

[0006] 此概述还描述了其他技术可如何得益于GVN,它们可作为使用GVN 的一些或全部组件的独立部署,或可被快速部署为在现有GVN之上的独立机制,从而利用它的益处。

[0007] 人类能够察觉到200毫秒或更高的延迟,因为这通常是人类对事件的平均反应时间。若延迟时间过高,诸如瘦客户端到基于云的服务器、客户关系管理(CRM)、企业资源规划(ERP)和其他系统等在线系统将运行不佳并且甚至可能由于超时而停止运行。高延迟时间加上高分组丢失可能导致连接不可用。即使数据通过,在特定时刻,过于缓慢会导致用户体验(UX) 不佳并且在这些情况下,用户最终可能拒绝接受这些状况,它们实际上会将送达不佳的服务视作无用。

[0008] 为了解决一部分这些问题,已经开发了各种技术。一种技术是WAN 优化,通常涉及局域网(LAN)边缘处的硬件(HW)设备,该设备建立通向另一LAN边缘处的另一WAN优化HW设备的隧道,从而在两个硬件设备之间形成广域网(WAN)。此技术假设两个设备经由稳定连接彼此连接。WAN优化器力求压缩并保护数据流,这通常会引起速度增益。采用WAN 优化的商业驱动器用以节省发送的数据容量,进而降低数据传输成本。该技术的缺点是它通常是点对点的并且当两个设备之间的连接不良时可能费力,因为对通过两者之间的互联网的流量路径的控制极少甚至没有。为了解决此问题,WAN优化器的用户通常选择在MPLS或DDN线路

或其他专用电路上运行它们的WAN,导致额外费用并且经常也必然会伴有刚性、固定的点对点连接。

[0009] 在撰写本专利时的市场中,一些供应商关注于销售硬件,而不关注他们的硬件设备之间的互联网上的连接服务。另外一些供应商是服务提供者,他们可能提供可由客户安装到客户自己设备上以连接至服务提供者的云服务器的简单端点设备或软件,作为连到供应商打包提供的服务的链路,但这些供应商的主要焦点是服务提供。

[0010] 直接链路例如MPLS、DDN、专用电路或其他类型的固定点对点连接可提供连接质量和服务质量(QoS)保障。这些链路是昂贵的并且由于需要从每一个连接侧的POP进行物理布线,通常需要花费很长时间来安装。当经由此直接连接的WAN从一个LAN内连接至另一LAN的资源时,点对点拓扑工作良好。然而,当通向一般互联网的网关(GW)位于LAN一端的LAN处,例如位于公司总部时,则来自子公司国家的远程LAN的流量可通过GW被路由至互联网。随着流量通过互联网返回到子公司所在的同一国家/地区的服务器,将出现减慢。流量随后必须从LAN通过WAN流到GW所在的LAN,然后通过互联网返回初始国家的服务器,随后通过互联网返回到该GW,并且随后沿着专用线路返回到LAN内的客户端设备。实际上,本应当只需一小部分的全局延迟时间来访问此附近站点,这样会导致访问该附近站点的全局传输时间加倍或者是三倍(或者更严重)。为克服此问题,配置适当改变并且附加了设备的另一互联网线路的替代连接性可在此系统的每一端将本地流量提供至互联网。

[0011] 建立从一个LAN至另一LAN的WAN链路的另一选项涉及在两个路由器、防火墙或等效边缘设备之间构建隧道,诸如IPSec或其他协议隧道。它们通常是加密的并且可提供压缩和其他逻辑来尝试改良连接性。对两点间的路由的控制极少甚至没有,因为它们依赖于互联网上的各种中间参与者的政策,这些中间参与者通过它们的网络传输自己的流量,并且与其他运营商和/或网络运营商为对等关系。防火墙和路由器、交换机以及来自若干设备供应商的其他设备通常具有内置到固件中的隧道选项。

[0012] 基于软件(SW)的虚拟专用网络(VPN)经由在客户端设备与VPN服务器之间的隧道提供隐私性。这些具有加密优点并且在一些情形下还提供压缩优点。但同样地,对在VPN客户端与VPN服务器之间以及在VPN服务器与主机服务器、主机客户端或目的地的其他设备之间的流量如何流动的控制极少甚至没有。这些通常是点对点连接,需要每个使用VPN的设备安装客户端软件并且需要一定的技术能力来维护每个设备的连接。若 VPN服务器出口点经由优质通信路径紧靠目的地主机服务器或主机客户端,则性能将为良好的。如果不紧靠,则将显著制约性能并且引起可用性方面的不满。VPN用户经常需要不得不从一个VPN服务器断开连接并重新连接到另一VPN服务器以相对于另一个区域的内容而言,优质地或本地接入来自一个区域的内容。

[0013] 全局虚拟网络(GVN)是在互联网之上的一种类型的计算机网络,它采用由先进隧道彼此安全链接的分布在世界各地的设备网提供全局安全网络优化服务;经由应用程序接口(API)、数据库(DB)复制、和其他方法协作并通信。始终经由由自动化系统驱动的高级智能路由(ASR)所管理的最佳通信路径进行GVN中的流量路由,所述自动化系统将构建器、管理器、测试器、算法分析和其他方法相结合,以适应随时间变化的条件和学习,以便配置和重新配置系统。

[0014] GVN在一个或多个常规互联网连接之上提供服务,以提供安全、可靠、快速、稳定、

精确和集中的并行连接性。这些益处通过数据流的压缩实现，该数据传输通过在ETO与紧靠EPD的接入点服务器(SRV_AP)之间的多个包装、伪装和加密隧道的连接。对EPD与SRV_AP之间的连接质量进行持续监测。

[0015] GVN是已安装软件(SW)的硬件(HW)端点设备(EPD)、数据库(DB) 以及GVN系统的其他自动化模块，例如中立应用程序接口机制(NAPJ顶)、反向通道管理器、隧道管理器，以及将EPD连接到诸如GVN内的接入点服务器(SRV_AP)和中央服务器(SRV_CNTRL)等分布式基础设施设备的更多特征的组合。

[0016] 算法持续分析当前网络状态，同时考虑到后续趋势加上长期历史性能，以确定要采取的最佳流量路由并且将流量推送到的最佳SRV_AP或 SRV_AP系列。配置、通信路径和其他改变是自动并且在传输过程中 (onthefly)进行的，所需的用户交互或干预极小或者为零。

[0017] EPD和SRV_AP中的高级智能路由确保了流量通过尽可能简单的 GVN的“第三层”，经由最理想的路径从起点流动到目的地的。连接至 GVN的客户端设备将该第三层视作正常的互联网路径，但与经由常规互联网流动到相同目的地的流量相比，它的跳跃数量较少、安全性更高并且在大多数情况下，延迟时间较短。逻辑和自动化在GVN的“第二层”操作，在所述第二层中，GVN的软件自动监测并控制虚拟接口(VIF)的下层路由和构造、多个隧道以及通信路径的结合。GVN的第三层和第二层存在于GVN的可操作的“第一层”之上，该第一层与底层互联网设备交互。

发明内容

[0018] 本发明公开了用于经由虚拟全局网络来连接设备的系统和方法。所述网络系统可包括与第一端点设备通信的第一设备。所述网络系统可包括与第二端点设备通信的第二设备。所述第一设备和所述第二设备可与通信路径连接。所述通信路径可包括将每个端点设备连接至一个或多个中间接入点服务器和一个或多个控制服务器的一个或多个中间隧道。

[0019] 根据本实施例的其他方面，所述第一端点设备和中间接入点服务器中的至少一个被配置用于执行域名系统(DNS)查询以定位所述第二设备。

[0020] 根据本实施例的其他方面，所述第一端点设备和中间接入点服务器中的至少一个被配置用于从高速缓冲存储器执行域名系统(DNS)查询以定位所述第二设备。

[0021] 根据本实施例的其他方面，所述中间接入点服务器中的至少一个被配置用于缓存内容。

[0022] 根据本实施例的其他方面，所述端点设备和中间接入点服务器中的至少一个被配置用于基于全局虚拟网络执行智能路由。

[0023] 根据本实施例的其他方面，所述智能路由基于最佳带宽、最低延迟时间、最少跳跃和无分组丢失中的至少一个。

[0024] 根据本实施例的其他方面，所述智能路由基于实时统计和历史统计中的至少一个。

[0025] 根据本实施例的其他方面，所述端点设备和中间接入点服务器中的至少一个被配置用于执行防火墙服务。

[0026] 根据本实施例的其他方面，所述防火墙服务在所述第一设备与所述中间接入点服

务器之间。

[0027] 根据本实施例的其他方面,所述防火墙服务在所述第一设备与中间接入点服务器和所述第二端点服务器之间。

附图说明

[0028] 为了便于更全面理解本发明,现在参考附图,在附图中,类似的元件采用类似的数字或参考符号进行标记。这些附图不应被解释为限制本发明,而旨在仅仅用于示例性目的。

[0029] 图1示出了由全局虚拟网络("GVN")使用并实现的技术的方框图。

[0030] 图2示出了互联网的高级别方框图。

[0031] 图3是示出经由域名系统(DNS)的统一资源定位符(URL)至数字互联网协议(IP)的解析的方框图。

[0032] 图4是示出将数据从主机客户端设备(C##)传输到另一主机客户端或主机服务器设备(S##)所采用的上游和下游路径的简图。

[0033] 图5是示出将数据从主机客户端设备(C##)传输到另一主机客户端或主机服务器设备(S##)所采用的路径中的边界交换的简图。

[0034] 图6示出了互联网上存在的一些示例威胁和问题。

[0035] 图7示出了内容传递网络(CDN)解析和区域特定内容的传递。

[0036] 图8示出了代理服务器的操作。

[0037] 图9示出了在两个网关设备之间建立的点对点隧道。

[0038] 图10示出了在设备范围、全系统范围、通信范围和设备协作之间的安全特征的关系。

[0039] 图11示出了全局虚拟网络的设备之间的信息流。

[0040] 图12描述了用于支持GVN中的一些设备的自动化的堆栈。

[0041] 图13示出了包括互联网或暗色光纤上的主干段的GVN拓扑。

[0042] 图14示出了在由GVN实现的云中的分布式防火墙(FW)。

[0043] 图15示出了由全局虚拟网络驱动的云中的多周界防火墙(MPFW)。

[0044] 图16示出了作为全局虚拟网络(GVN)的一部分共同工作的三种类型的网络设备的软件架构的逻辑视图。

[0045] 图17示出了使用具有主干段和八角形路由的轴辐式(hub andspoke)拓扑的GVN。

[0046] 图18示出了在北美、欧洲和亚洲的一些GVN全局节点与其对应服务区之间的主干连接。

[0047] 图19示出了在GVN内的各个设备之间的连接性。

[0048] 图20示出了GVN模块和设备的交互方式。

[0049] 图21示出了关于GVN模块和设备之间的交互方式的额外细节。

[0050] 图22示出了GVN模块和设备在互联网上与其他设备的交互方式。

[0051] 图23示出端点设备(EPD)与接入点服务器(SRV_AP)之间的多个隧道连接性。

[0052] 图24是当今互联网的工作原理的简化示例图,其中考虑到跳跃计数或生存时间(TTL)以及由于对等关系和相关路由政策采取的路径。

[0053] 图25示出了用以增强性能的基础设施的策略定位。

[0054] 图26示出了GVN结合诸如网络弹射(NetworkSlingshot)等技术的方式。

[0055] 图27示出了在各种GVN设备的数据库中的表如何彼此相关。

[0056] 图28示出了在各个模块、机制、技术和GVN其他组件之间的协作成果。

[0057] 图29示出了GVN的高级智能路由(ASR)特征。

[0058] 图30示出了在客户端(C)与服务器(S)之间建立一系列加密隧道。

[0059] 图31示出了对等体对中的两个对等体所需的信息流。

[0060] 图32至图35示出了相对于GVN隧道的中立性和安全性的GVN的第三层。

[0061] 图36示出了将多个网络结构共同编织成网络毯式框架(Tapestry)。

[0062] 图37示出了GVN中用于自动设备协作的通信路径。

[0063] 图38示出了动态隧道建立的问题和挑战。

[0064] 图39示出了经由两个或更多个EPD将两个LAN桥接为广域网 (WAN)。

[0065] 图40示出了在GVN上运行的多周界防火墙机制(MPFWM)。

[0066] 图41示出了建立在互联网顶部之上(OTT)的GVN堆栈。

[0067] 图42将互联网协议IP堆栈、OSI模型和GVN网络堆栈进行比较。

[0068] 图43示出了国家之间经由众多可能路由的全局互联网流。

[0069] 图44将互联网协议IP堆栈、OSI模型和GVN网络堆栈进行比较。

[0070] 图45示出了两个LAN之间经由GVN的隧道。

[0071] 图46示出了GNV层1、层2和层3操作。

[0072] 图47示出了高级智能路由(ASR)特征以及端点设备(EPD)内的GVN 的地理目的地机制的元素。

[0073] 图48示出经由GVN采取的多个并行型流量路径的示例。

[0074] 图49描述了从一个设备到第二个设备的自动高级智能路由(ASR)。

[0075] 图50示出了低于周界的BB/主干层与高于周界的IP/互联网层之间的安全周界。

[0076] 图51是全局虚拟网络(GVN)内的高级智能路由(ASR)的流程图。

[0077] 图52是通过GVN从起点到目的地可用的各种路由的流程图。

[0078] 图53是控制从起点设备到端点设备的流量路由选择的算法的流程图。

[0079] 图54示出了GVN中的自动设备协作和信息交换所需的模块。

[0080] 图55示出了经由GVN的中立API机制(NAPIM)的EPD、SRV_CNTRL和SRV_AP之间的通信。

[0081] 图56示出了经由NAPIM的GVN设备之间可用的各种类型的通信。

[0082] 图57描述了全局虚拟网络(GVN)内的不同类型设备之间的API调用组。

[0083] 图58描述了从客户端设备发起,通过发送到服务器设备并返回客户端的API调用所采取的步骤。

[0084] 图59是示出EPD与SRV_AP之间用于获得地理目的地功能性的交互的流程图。

[0085] 图60描述了地理目的地内的设备协作。

[0086] 图61示出了全局分布的平行文件系统(PFS)在GVN内的操作方式。

具体实施方式

[0087] 概述

[0088] 图1示出由全局虚拟网络(“GVN”)使用和实现的技术的方框图,所述全局虚拟网络包括GVN核心元件G0、GVN模块G100和由全局虚拟网络GVN实现的技术G20CLGVN核心包括机制概览G1以及它的构成部分,即拓扑G2层、构造G3层、逻辑G4层和控制G5层。GVN核心G0 还包括相对于GVN元件G6以及与这些GVN元件之间的关系。

[0089] GVN可包括插件和/或独立GVN模块G100,所述模块包括但不限于:PCT/US16/12178中所述的中立API机制(“NAPIM”)模块G102; PCT/US15/64242中所述的地理目的地(“Geo-D”)模块G104;美国临时专利申请US62/151,174中所述的高级智能路由(“ASR”)模块G106、连接模块G108和其他模块G110。

[0090] GVN还提供可实现其他技术的平台,所述技术包括但不限于:网络毯式框架(NetworkTapestry)G202;MPFWMG204;网络弹射 (NetworkSlingshot)G206;网络信标G208、信号粒度 (Granularityofatick)G210和其他技术G212。这些在美国临时专利申请第 62/174,394号、美国临时专利申请第62/266,060号中描述。

[0091] GVN模块(G100)和由GVN实现的技术(G200)可作为GVN的构成部分在现有GVN之上操作,或可为独立的并且采用GVN的所有或一些分离部分来支持其自身的独立操作。

[0092] 图2示出了互联网的高级别方框图。一般用户对互联网如何运作的理解非常粗略。主机源2100是起点并且表示客户端设备,所述客户端设备可以是计算机、移动电话、平板设备、膝上型计算机或其他此类客户端。此客户端经由互联网2200连接至主机服务器2300以发送或检索内容,或连接至另一主机客户端2303以发送或接收信息。

[0093] 技术知识较低的用户可能会认为流量是沿着路径2P002到达主机服务器的,甚至不了解他们的数据将会通过互联网中转。或者,他们可能认为流量经由路径2P006直接流至另一客户端设备。

[0094] 对互联网如何运作的了解更多的用户会理解,流量经由路径2P004流至互联网2200,并且随后经由路径2P102流至主机服务器目标2300或经由路径2P104流至主机(客户端)目标2302。

[0095] 了解更多技术知识的用户将进一步理解,当发送电子邮件时,此电子邮件将离开其客户端设备2100,经由路径2P004传输至互联网2200并且随后经由路径2P202传输至电子邮件服务器2202。随后电子邮件的接收者将经由其主机客户端2302,沿着到达互联网的路径2P104,然后沿着到达邮件服务器2202的路径2P204请求取回该电子邮件。

[0096] 一般人对互联网的了解程度大约就是这样。

[0097] 图3是示出经由域名系统(DNS)的统一资源定位符(URL)至数字互联网协议(IP)的解析的方框图。

[0098] 作为文件或数据流或数据块的从主机客户端(C)3100到主机服务器 (S)3300的内容请求3000或推送从主机客户端(C)3100流至主机服务器(3) 3300。响应或内容传递3002作为文件或数据流或数据块从主机S返回到主机C。与主机服务器(S)成客户端-服务器(CS)关系的主机客户端设备 3100请求访问来自远程主机服务器(S)的内容或经由统一资源定位符(URL) 或其他网络可达地址将数据发送到远程主机服务器(S)。

[0099] 从主机客户端(C)3100至互联网3206的初始连接示出为3P02,即从主机客户端(C)至可直接面对的存在点(POP)3102的连接。在其他情形中,主机客户端(C)可位于局域网(LAN)中,所述局域网随后经由存在点(POP) 连接至互联网并且可被称为最后一英里连接。

存在点(POP)3102表示服务供应商(ISP)经由它们的网络和互连提供的从端点到互联网的连接。这可以是但不限于电缆、光纤、DSL、以太网、卫星、拨号和其他连接。若 URL是域名而非数字地址,则将此URL发送至域名系统(DNS)服务器 3104,在该服务器中,出于路由目的将域名转换为IPv4或IPv6或其他地址。

[0100] 从主机客户端(C)3100至主机服务器⑶3300的流量通过互联网3206 路由,这表示POP(3102和3302)之间的传输,其中包括对等、回程或网络边界的其他传输。

[0101] POP3102与域名系统3104之间用以从统一资源定位符(URL)查找数字地址以获得IPv4地址或目标服务器(S)的其他数字地址的连接3P04可直接访问从POP或经由互联网3206访问。从ISP的POP3102至互联网3206的连接3P06可为单宿主或多宿主连接。相似地,从互联网3206至远程ISP的连接3P08也可为单宿主或多宿主连接。此连接一般是连接到 ISP或互联网数据中心(IDC)的面向互联网的POP3302。从远程ISP的 POP3302至主机服务器(S)的连接3P10可为直接的或经由多个跳跃。

[0102] 经由域名系统进行的从URL或主机名至数字地址的查找是目前互联网上的标准,并且系统假设DNS服务器是一体的并且DNS服务器结果是当前结果并且可信任。

[0103] 图4是示出将数据从主机客户端设备(C##)传输到另一主机客户端或主机服务器设备(S##)所采用的上游和下游路径的简图。诸如C01或S08 等设备标签中所用的数字是用于定位各个设备的标识目的,并且数字本身不意指或暗示一个设备比另一个设备更大或具有更大功率。

[0104] 图4示出主机客户端设备(C##)、主机服务器设备(S##)、交换机 (SW##)、路由器(酬、区域路由器(RR##)、边缘路由器_#)、核心路由器 (CR##)。通信路径或管道(P##)是指两个设备之间的连接并且线路厚度用以表示管道的大小或带宽容量。线路越薄,每秒兆位(Mbp)越低。线路越厚,每秒Mbp或千兆位(Gbp)的量越高。P##的距离并非按比例绘制并且当提及设备间的P##时不考虑跳跃计数或生存时间(TTL)和延迟时间或往返时延(RTT)。

[0105] 简化局域网(LAN)在交换机(SW)SW01的下游。它由连到客户端设备C01和C04的电线连接P01和P04组成。无线连接用无线集线器 WLAN01与无线客户端设备C02和C03之间的虚线P02和P03表示。

[0106] LAN与其互联网服务供应商(ISP)的存在点(POP)R01之间的连接 P05还可被称为“最后一英里”。此POPR01是将其他辐条P06、P07、P08 和P09连接至诸如SW02、SW03、SW04和SW05等其他客户端的对应交换机的中心。还存在通向区域路由器(RR)RR02的上游路径P16。

[0107] 这种轴辐式(hubandspoke)拓扑被图示成用于POPR02、R03和R04,它们与相应交换机(例如,3需6、5需7、5需8、5需9、5110、5111、 5112、5113、5114、5115、5116、5117、5￥18、SW19、SW20)的轮辐连接 ^1^n,P10、P11、P12、P13、P14、P15、P51、P52、P53、P54、P55、P56、P57、P58、P86)以及它们与至其区域路由器(例如,RR02、RR03、RR04、 RR05)的连接(例如,P17、P18、P46、P28)。

[0108] 从区域路由器RR02至边缘路由器ER02的进一步上游连接P19描述了通向ISP网络的边缘路由器的连接。边缘路由器ER02具有通向核心路由器CR03的链路P20。这可被认为是互联网的主干。CR01与CR02之间的链路P32可描述非常大型的主干,所述主干被称为回程网络或当连接多个国家网络时可被称为国际回程网络。

[0109] POPR01和R02均被连接至区域路由器RR02并且这可表明但不限于这两个POP位于

相同ISP的网络内。

[0110] 对于路由器R01网络内的设备与路由器R04网络内的设备之间的连接性，流量将采用许多可能路径中的一个路径，诸如 P16->P19->P20->P30->P31->P24->P27->P28。这可能描述两个或更多个不同ISP的网络之间的连接性对等，并且它们的中间潜在地存在其他运营商对等点，具体取决于流量传输通过的基础设施的拥有者。通过主干的流量将由潜在最高容量管道传输。路由器R01与路由器R04之间的流量还可经由路径P16->P41_>P44->P23->P27->P28传输。尽管该路径可能看起来更短，但是由于管道大小、中间设备、中间ISP的对等关系和政策，该第二路径在控制边缘路由器ER03以在两个其他ISP之间进行流量传输方面的效率可能最低。它们之间还可能存在隘口点。

[0111] 图示的另一特征是连接至交换机SW13的主机服务器S08至S12的连接性。这可在互联网数据中心(IDC)中或在LAN中。交换机SW13同时经由P53连接至路由器R03并且经由P46连接至区域路由器RR04。连接 P46可描述用于增强连接性的租用线路或直接数字连接。

[0112] 此图中示出的另一特征是P32位于路径可达到的最上游处，并且独立主机设备位于路径可达到的最下游处。核心处理器CR04、CR06和CR07 的下游是连接至区域路由器RR##的边缘路由器ER##，所述区域路由器向下连接至位于POP中的路由器R##。

[0113] 可能存在本文中未作描述的其他可能性并且事实上，每个路由器R## 具有通向交换机SW##的多个辐条并且设备之间存在大量更多管道P##。序列中还可能存在更多层等效区域路由器RR##或边缘路由器ER##设备或其他设备。

[0114] 图5是示出将数据从主机客户端设备(C##)传输到另一主机客户端或主机服务器设备(S##)所采用的路径中的边界交换的简图。这可与图4非常相似，但有一个例外。在核心路由器CR01与核心路由器CR02之间的主干上，在它们之间的对等路径上的特定点处存在一系列边界交换机400，这些交换机中的每个交换机相对于主干作为一个整体的容量有限，并且这些交换机之间可能存在拥塞事件。

[0115] 图6示出了互联网上存在的一些示例威胁和问题。图中已经简化了网络数据路径，以对连接性进行概述，并且重点说明来自端点设备(EPD)的威胁和来自中间设备的其他威胁。

[0116] 来自主机客户端设备C002的从主机服务器设备207检索内容请求应采用路径P109->P105->P103->P102->P101并且经由互联网101传输至 CP01->CP02->P205->P207。合法的互联网数据中心(IDC)可能存在负载平衡器，所述平衡器将流量发送至健康的主机服务器207(经由P207)或被感染的主机服务器206(经由P206)。被感染的主机服务器可能将恶意软件或病毒或其他不良内容发送回客户端设备C002。

[0117] 另一威胁是将合法流量重定向至被骗主机服务器114。流量应采用上文所述的C02与207之间的路径，然而被骗服务器可吸走合法流量。流量将仍采用诸如P109->P105->P103->P102->P101等路径并且通过互联网 101，但流量不会经由CP01传输到合法服务器，而是经由P113至P114 传输至被骗服务器114。

[0118] 被骗服务器可被设计用于通过对互联网用户看起来像真实服务器而对保密信息或凭证或其他数据进行钓鱼攻击。一般用户无法区分合法服务器与被骗服务器。第三方还可能使用被骗服务器通过发送回无效流量或已更改内容来阻止将合法流量传输到客户端。

[0119] 公共域名系统(DNS)服务器可用在互联网上以由客户端设备查询，进而将统一资

源定位符(URL)例如域名www.thisdomain.com转换为数字IP 地址例如IPv4或IPv6地址,以便来自主机客户端设备的流量可找到通向主机服务器设备的路径。

[0120] 若诸如212或116等DNS服务器中毒112或被骗114,则转换的数字 IP地址可能成为被送到非法的或被破坏的目的地设备的不正确引导流量。DNS可在互联网上被破坏的另一方式是设备不传递结果或传递不正确结果而不当操作。将变化从主DNS注册服务器传播到DNS服务器还需要清楚有效的连接性,否则索引结果可能变得丧失时效或错误。将通过安全DNS(DNSSEC)服务器110及其经由P19的连接性来说明如何保护DNS查找及使DNS查找安全的示例。这依赖于客户端设备连接至DNS服务器110 并且它们的“握手”不被中断的能力。

[0121] 即便当主机客户端和主机服务器设备均正确操作时,由于互联网未加密,仍存在非常真实的风险,即插入通向诸如邮件服务器203等主机服务器的通信路径中的中间点的嗅探器或拦截设备204可能截取并捕获数据。尽管送往邮件服务器203的流量应从互联网201经由P202到POP202到 P203路径流到邮件服务器203,嗅探器或拦截设备204将经由P204使得流量通过该204并且送往P222。非常难以检测此类干扰,除非能够确切地将通信路径中的跳跃的IP地址识别成属于恶意设备,而不是作为互联网基础设施的一部分的另一路由器。

[0122] 一个日益增长的威胁来自由一组感染设备213、215、216构成的BOT 网络,所述感染设备由诸如214等命令和控制(C&C)服务器控制。这些设备可共同地执行批量攻击,例如分布式拒绝服务(DDoS),其中主机服务器设备可能被大量涌入它们容量中的过多请求淹没,导致分离出来自合法主机客户端设备的请求变得缓慢或者完全无法解析。

[0123] BOT网络还可用以在C&C服务器的协调下执行秘密黑客攻击,因此与来自单一IP地址的相同攻击相比,尝试词典密码攻击的大批不同来源的IP地址将更难以完全阻止。

[0124] BOT网络还是用于垃圾(SPAM)电子邮件、钓鱼电子邮件、恶意软件分布和其他恶意目的的分布机制。

[0125] 诸如304等国家防火墙会阻止自由信息流。这些防火墙可用作阻止国家认为不良流量的审查工具。它亦可用作暗地窃取工业、商业或其他机密的拦截设备。根据当日时间、总互联网流量和这些国家防火墙的健康状况,传输通过它们的流量可能遭受延迟时间或分组丢失,或者被成形为最大带宽进而形成瓶颈,或者以上全部或甚至其他问题的组合。

[0126] 上文提及的示例实施例仅描述了一些问题和威胁。还存在许多其他威胁,并且不时会出现新的威胁。

[0127] 图7示出了内容传递网络(CDN)解析和区域特定内容的传递。内容传递网络(CDN)可在速度和灵活性方面提供显著优点并且当将内容提供至客户端时提供负载平衡。内容请求7REQ000从主机客户端(C)7100流至主机服务器(3)并且内容传递的应答流7RESP002作为文件或数据流或数据块从主机服务器(S)返回到主机客户端(C)7100。

[0128] 主机客户端(C)7100可以是设备,诸如膝上型计算机、桌上型计算机、电话、平板设备或用作与主机服务器(S)成客户端-服务器(CS)关系的客户端的其他设备。主机客户端(C)请求经由统一资源定位符(URL)来访问主机服务器(3)提供的内容。

[0129] POP7102、DNS服务器7104、互联网7300以如上文所述的常规方式操作。

[0130] 在CDN基础设施的情形中,CDN映射标记7200与CDN控制服务器 7202协调操作。CDN映射标记7200和CDN控制服务器7202确定主机客户端设备所在的区域以及针对提供的内容

主机客户端应连接至哪一⑶N 服务器。例如，如果主机客户端7100在区域A中，它将经由区域A中的服务器POP7404被路由至区域A中的⑶N服务器7504。区域B中的主机客户端7100将经由区域B中的服务器POP7402连接至区域B中的⑶N服务器7502。区域C中的主机客户端7100将经由区域C中的服务器POP7400 中的服务器的POP连接至区域C中的⑶N服务器7500。

[0131] 经由7P00、经由POP7102、经由7P004的初始CDN映射标记7200 查找可能非常快速，或者如果CDN映射标记服务器位于远离客户端设备的区域中，则可能花费相对高的查找时间。一旦完成查找，流量将经由 7P008流至最近和或最佳可用⑶N服务器。

[0132] 为了说明此图，将区域定义为不同于另一地理区域的地理区域。它不一定表示大的面积但可能具有大面积，并且它还可表示从一个区域至另一区域的大距离或它们可非常接近于彼此。关键是一个区域中的客户端将经由来自该区域而不是来自另一个区域的CDN服务器接收内容。

[0133] 在本示例实施例中，每个区域的内容与其他区域的内容不同。CDN 服务器7500、7502和7504与源服务器7600之间的是内容区域服务器 7700、7702和7704，这些内容区域服务器将区域特定内容发布到每个区域中的CND服务器，并随之将其提供给它们的对应区域中的客户端。

[0134] 当一个区域，例如区域C中的客户端7100想要获取由来自另一区域的服务器7502或7504提供的内容时，无论它们做了什么，都仅向所述客户端提供来自它们所在区域中的服务器7500的内容。它们不能访问其他内容，即使它们尝试强制连接至它们期望从中接收内容的区域中的内容服务器。它们不断从所在区域获取内容而不进行选择。局部DNS查找7104 解析仅指向所在区域的CDN服务器7500的IP。这可由于全局IP地址仅映射至所在区域中的⑶N(在全局IP的情况下)或另一原因。结果是客户端可能在7P404或7P402被地理阻止。

[0135] 基于当前地理位置的经由7P008的正常连接不会被阻止，并且流量以使主机客户端7100经由主机服务器7500接收该地理位置的内容的方式流动。

[0136] 针对与当前地理位置7502和7504不同的目标，流量在7P402和/或 7P408处停止并且主机客户端被来自远程地理目的地的内容拒绝。它们可能被迫连接至在它们当前位置7500中的服务器，或者不接收任何内容或者接收错误消息或仅不期望内容，这具体取决于CDN控制系统7202的配置和政策。

[0137] 图8示出了代理服务器的操作。内容请求或推送8REQ000作为文件或数据流或数据块从主机客户端(C)流至主机服务器(S)。内容传递 8RESP002作为文件或数据流或数据块从主机服务器(S)返回主机客户端 (C)。主机客户端8100，即与主机服务器8500成客户端-服务器(CS)关系的客户端设备，请求经由统一资源定位符(URL)从远程服务器(S)访问内容。此请求将通过运行代理客户端软件的网关(GW)设备8102。在其他情况下，代理客户端软件可直接在主机客户端8100上运行。代理客户端软件经由加密或未加密的隧道连接至代理服务器8306、经由路径8P02从网关GW8102连接至存在点(POP)8200、经由路径8P04连接到WAN8308(互联网的一部分)、经由路径8P6连接到远程区域中的代理服务器8306。流量从代理服务器8306离开、经由路径8P16进入开放互联网8300并且经由路径8P12连到POP8302并且随后经由路径8P10而连接至目标区域中的主机服务器8500。

[0138] 主机服务器将该流量视为来自代理服务器的IP地址和地理位置。如果所述IP处于由目标区域中的服务器限定的相同区域中，将会提供期望内容。为了帮助此本地化，代理服

务器将通常连接至与代理服务器处于相同的区域中的DNS服务器8404。

[0139] 图9示出了两个网关设备9A1与9B1之间建立的点对点隧道TUN。每个设备9A1和9B1位于互联网EH3至H115与它们对应的局域网 (LAN)9A2和9B2之间的边缘9EDGE-1和9EDGE-2处。

[0140] 从H11至EH17的基线描述了点对点的跳跃数量。从H13至EH15 的跳跃数量是假定的并且出于说明目的提供,而且现实连接路径中的跳跃数量可能更多或更少。采用隧道9TUN的客户端从9A2至9A1至9TUN 至9B1至9B2的跳跃数量将为约四或五个可见跳跃。

[0141] 本示例实施例描述了LAN9A2通过其网关9A1连接至一个互联网服务供应商9ISP-1的网络并且LAN9B2通过其网关9B1连接至另一互联网服务供应商9ISP-3的情景。本示例实施例进一步说明了9ISP-1不与9ISP-3 直接对等。9ISP-1和9ISP-3两者要求它们在两个方向的网络流量必须传输通过另一互联网服务供应商91SP-2的网络。91SP-1与91SP-2之间的互连被定义为对等点9PP-01并且从9ISP-3至9ISP-2的互连被定义为 9PP-02。

[0142] 本示例实施例的点用于示出在互联网上,第三方互联网服务供应商或诸如主干或回程供应商等同等供应商通常会传输其他互联网服务供应商的流量。9ISP-1或9ISP-3对9ISP-2如何传输它本身的流量具有很少以至几乎没有控制。尽管9ISP-1的客户9A2能够直接向他们的供应商9ISP-1 投诉服务问题并且9B2可直接向9ISP-3投诉,但是如果问题是关于 91SP-2,那么9A2或9B2几乎无法做任何事情来直接影响91SP-2。

[0143] 潜在拥塞点可能出现在任何设备上,但是由于9PP-01和9PP-02是对等点,因此它们是关注区域。对全部连接的路由和服务质量的控制有限。因此,点对点隧道可能难以在距离上维持高质量、稳定连接,特别是在存在部分流量传输通过第三方网络时。

[0144] 图10示出了在设备范围1080与全系统范围1090之间的安全特征的关系。它还指出通信范围1098和设备协作1089。

[0145] 关于设备范围1080,GVN保护其数据的客户端隐私性、网络数据流、凭证、对等体对信息,并且保护物理设备免受遭受入侵,其中所包括的专有代码免于遭受篡改或窃取,以及其他威胁。

[0146] 全系统范围1090需要保护不受入侵或诸如DDoS攻击等其他恶意流量,防误操作,进行围绕次优设备或路径的路由,平衡和分散负载并且防止耗尽资源、IP地址或其他全局问题。

[0147] 通信范围1098的重点在于主要通过流量隧道TUN而推送通过GVN 的流量途径。它还覆盖在GVN的外部网络与内部网络之间的出入点(EIP)。它可防止流量劫持、中间人攻击、中毒信息源(诸如不良DNS等等)以及其他威胁。此外,对各个网络分段的质量和其性质的测试使GVN能够理解完整路径QoS并且绕过问题。

[0148] 设备协作1089安全特征处于适当位置以保护GVN内的各个设备的操作完整性。安全返回通道、抗入侵机制、DNS安全网、诸如旋转按键等各种数据库保护、中立API机制(NAPIM)、自动测试、更新、对等体对关系、验证和其它模块可确保维持系统完整性。

[0149] 图11示出了全局虚拟网络的设备之间的信息流。由数据库B200和文件存储器HFS200构成的中央存储库驻留在中央服务器(SRV_CNTRL)200 上。

[0150] 标记为P###的设备之间的通信路径可以表示API调用、数据库复制、直接文件转换、诸如通过API调用的数据库复制等组合或者其他形式的信息交换。较粗的线11P200100、

11P200300、11P200500、11P100200、 11P100300、11P10011500、11P300200、11P300500、和11P500200表示具有对等体对的GVN设备之间的通信并且彼此之间特权关系。

[0151] 图中示出了从SRV_CNTRL 200经由11P200100到EPD100，从 SRV_CNTRL200经由11P200300到SRV_AP300，或从SRV_CNTRL200 经由11P200500到其他设备11500的循环模式的对等体对通信。EPD100 经由11P100200与SRV_CNTRL200通信、经由11P100300与SRV_AP300 通信，并且经由11P1001500与其他设备11500通信。

[0152] 在一些情况下，设备会共享信息环路，诸如EPD100可以经由 11P100200向SRV_CNTRL200请求信息，并且该请求将经由11P200100 发回到EPD100。

[0153] 在其他情况下，一个设备可以报告与其他设备相关的信息，诸如 SRV_AP 300经由11P300200向SRV_CNTRL200报告，而 SRV_CNTRL200随后经由11P200100将信息发送到EPD100和 SRV_AP300，并且经由11P200300将信息发送到发出报告的SRV_AP300 以外的其他SRV_AP300，并经由11P200500将信息发送到其他设备11500。

[0154] 在其他情况下，无需完整环路，诸如从诸如EPD100等设备经由 11P100200将日志记录信息发送到SRV_CNTRL200，不需要进一步转发这个信息。然而，日志记录信息可能之后经由11P200500从SRV_CNTRL200 上的存储库移动到长期日志记录存储服务器11500。

[0155] 设备EPD100与SRV_AP300之间存在直接链路11P100300。直接链路11P300500是从SRV_AP300到其他设备11500。直接链路涉及设备之间不需要SRV_CNTRL200参与的通信。

[0156] 来自SRV_CNTRL200的推送信息可以是经由11P306发布的RSS馈入信息或其他类型的信息。来自SRV_CNTRL200的API可以是传统API 事务，也可以是经由11P302REQ发出请求并经由11P302RESP接收响应的RESTfulAPI调用。呈现的推送信息和API元素用于示出不共享对等体对关系、特权状态的设备和/或具有GVN设备的相似系统架构。

[0157] 图12描述了用于支持GVN中一些设备的自动化的堆栈。具体来说，此图示出了自动化设备协作和联网以及操作系统(O/S)管理所需要的模块。

[0158] EPD100是端点设备。SRV_AP300是位于目标目的地区域中的接入点服务器。SRV_CNTRL200是可由EPD和SRV_AP二者以及由可支持图形目的地机制的其他设备或者其他GVN模块、组件或服务器访问的中央控制服务器。

[0159] 每个设备EPD100、SRV_AP300和SRV_CNTRL200将关于它们本身的信息以列表、文件、数据库表和记录的形式以及以其他方式储存在本地信息存储库中。此存储库还包括关于对等体设备关系、储存日志记录的信息以及其他相关操作信息。SRV_CNTRL200还具有额外储存功能并且它的作用是向与其相关的其他设备和/或向可能与其连接的对等体设备提供信息，以便评估当前状态并且提供类似于集中控制的指导，例如发布服务器可用性列表和其他功能。中立API机制(NAPM)可在设备与这些设备的相连对等体之间发送信息，并且还可用以更新API本身。

[0160] SRV_CNTRL200上的数据库S293用作该设备本身的相关信息的存储库以及其他设备的中央存储库。许多位置中可能有许多不同 SRV_CNTRL200服务器来充当多主设备。每个数据库可以储存特定信息，包括隧道信息、对等体信息、流量信息、高速缓存信息和其他信息。安全性和其他方面由每个设备独立管理，包括心跳功能、触发脚本和其他机制。

[0161] GVN软件D196、D296、D396包括隧道构建器/管理器、虚拟接口管理器、自动智能路由、测试模块、安全、日志记录和其他功能。图11还示出了操作系统(O/S)级数据包D195、

D295、D395并且包括硬件和软件驱动程序、驱动程序、安装的数据包，包括它们的从属软件数据包，以及系统硬件组件之上构建的其他项目。

[0162] 图13示出了包括在互联网或暗色光纤上的主干段的GVN拓扑。标题为“用于从远程网络区域检索内容的系统和方法”(SYSTEMANDMETHODFORCONNTENTRETRIEVALFROMREMOTENETWORKREGIONS)的国际专利申請第PCT/UJS15/64242号(中公开了一种特征，其中多个文件被聚集成较大文件并且经由“链式高速缓存”通过文件传输从一个地理区域发送至另一地理区域。为/实现这一有利特征，文件传输需要尽可能快。作为多种数据有效负载“文件”群组的传输方法，本发明的信息弹射(informationslingshot)方法与先前技术的方法相比，更快速地将较大的数据块从世界一端移动至另一端。

[0163] 参见图13，示出了多个区：LAN区0(ZL00)、LAN区1(Z110)、互联网区0(ZI00)、互联网区1(ZI10)、互联网区2(ZI20)、互联网区3(ZI30)、互联网数据中央区2(ZD20)以及互联网数据中央区3(ZD30)。

[0164] 区域或区ZD20中的SRV_BBX1372可通过暗色光纤13220经由暗色光纤连接13P220连接至另一区域或区ZD30中的SRV_BBX1380。SRV_BBX1372经由13P220、绕过SRV_BBX堆栈1380并且经由路径 13P82经由远程直接记忆装置存取(RDMA)将文件直接写入至平行文件存储器PFS1382oSRV_BBX1380使用本发明来经由13P220、绕过SRV_BBX 堆栈1372并且经由路径13P74经由远程直接记忆装置存取(RDMA))将文件直接写入至平行文件存储器PFS1374。

[0165] 路径13P210可为IPv4或某种标准化互联网协议，流量通过这些标准化互联网协议经由隧道或其他类型通信路径经由GVN之上的路径13P210 从SRV_AP13300流至SRV_AP13310和/或从SRV_AP13310流至 SRV_AP13300。

[0166] 这表明，各种类型网络结构可组合成更大的网络毯式框架(Tapestry)。这些结构可无缝地编在一起，如美国临时专利申請第62/174,394号中所述。这可以是独立方法，也可以集成为由多个网络分段构成的较大网络路径内的网络分段。本示例实施例示出了全局虚拟网络(GVN)、其多个设备、通信路径和其他实施例的拓扑。它示出了各种地理区域或区或地区如何通过各个类型路径而链接在一起。

[0167] 图14示出了在由GVN实现的云中的分布式防火墙(FW)。由于GVN 的拓扑、设备到设备通信和安全流量路径的性质，防火墙机制可基于云并且还可以是虚拟化的。凭借经由开放互联网14000的出入点(EIP)流至和流自GVN的面对防火墙的跳跃144，可以存在云防火墙(CFW)负载平衡器 144LB，所述CFW负载平衡器能够分配诸如144-2、144，3等云防火墙资源等。

[0168] 这种按需提供的可缩放性为GVN客户端提供了众多优点。通过消减云中即将遭受的威胁的攻击命中率，客户端的“最后一英里连接性”不受影响。与控制节点和分析器相结合的该云防火墙使遭受攻击的区域中的 FW能够感知攻击的性质、来源、标记和其他特征，以便云防火墙能够在目标转移时意识到并准备抵御攻击。此外，关于过去和当前攻击的信息可经由GVN的中立API机制(NAPM)共享至其他CFW实例，以使能够感知全局威胁。这还提供同时运行多种类型FW机制的优点，如参考图15所述。

[0169] 图15示出了由全局虚拟网络驱动的云中的多周界防火墙 (MPFW)AVN隧道15TUNO在端点设备(EPD)15100与紧靠EPD15100的接入点服务器(SRV_AP)15300之间的互联网顶部

之上(overthetop,OTT)。

[0170] 本示例实施例中指出的三个周界是:15M1,它表示客户端位置与其通向互联网的链路之间的边界;15M2,它是云中紧靠SRV_AP15300的数据中心处的边界;以及15M3,它是与SRV_AP15300处于相同数据中心处或紧靠SRV_AP15302的另一位置处的另一边界。

[0171] 隧道15TUN2与15TUN0是相似的,而在一个方面中有所不同,SⅡ,它连接的个人端点设备(PEPD)15130可能是移动式设备,因此通过公共接入无线或有线或其他网络连接至SRV_AP15300以集成到GVN中。

[0172] 每个SRV_AP15300和SRV_AP15302可表示可经由一个或多个隧道与EPD15100和/或EPD15130同时连接的一个或多个SRV_AP设备。

[0173] 在本示例实施例中描述了三种类型的防火墙。FW本地15442是客户端可用以保护其局域网(LAN)不受基于互联网的威胁的示例防火墙。这通常位于EPD15100与LAN15000之间。此FW15442可提供诸如IP地址和端口阻塞、转发以及其他功能等特征。所示出的其他两种类型的防火墙是提供状态分组检查(SPI)的位于15M3的FWSPI15446以及提供深度分组检查(DPI)的位于15M2的FWDPI15444。

[0174] 在SPI与DPI之间的差异涉及到性能与可见度之间的权衡。SPI检查分组标头处以查找恶意信息或查找图案,或者将来自已知威胁列表的IP 地址或端口或其他信息与当前的分组流进行匹配。从名称中可看出,DPI 更深度地查看整个分组,并且在多部分、多分组传输的情况下,它将会查看对一系列分组的编译以便进一步了解所传输的数据。

[0175] 所有防火墙可以被配置用于调查并且对传入和传出流量应用规则,并且提供其他相关的功能性。在许多情况下,客户端将必须在SPI的效率与 DPI的彻底但耗费资源和时间的需求之间做出选择。

[0176] GVN提供将这些FW分布于云中的多个点的机会。并且对于要彼此前后紧接着操作的各种类型的防火墙,还不妨碍流量流。

[0177] 通过经由远程EIP15310将FWSPI15446定位在15M3,即互联网15302 的最近边缘处,可以抵御来自已知源IP地址或具有已识别的恶意标头的大量攻击流量。流量从SRV_AP15302经由15T10流至FWSPI15446并且经由15T12返回。FWSPI15446可以是具有大量需求资源的CFW负载平衡器(参见图14)。15113处的SRV_AP可以是具有巨大容量的多宿主主干。因此,在第一周界处,可捕获攻击,从而保护GVN中的带宽。

[0178] 在下一周界15M2处,FWDPI15444可使全部流量流过或仅经由15T20 从SRV_AP15300接收流量副本,并且可能或可能不经由15T22返回流量。重点在于DPI特征可以是允许特定流量通过但分析并记录结果的后缘指示器。此FWDPI15444还可以是CFW,所述CFW在需要时采用根据需要提供的资源进行负载平衡,以在需要时应付大规模的事件,而不需要使各个客户端必须处理或承担用于在正常期间维持基础设施的成本负担。

[0179] 来自FWSPI15446和FWDPI15444的信息经由内部通信路径15P6彼此共享,所述内部通信路径可由GVN的NAPM或通过GVN隧道或通过 GVN返回隧道或经由其他通信途径传输。每个FW机制还与GVN的中央控制服务器(SRV_CNTRL)15200共享信息。此信息可以在中继至世界范围内的其他FWSPI和FWDPI,以使得数据库中可提供攻击矢量、来源、有效负载和其他相关信息,从而使得SPI和DPI检查可以具有用于比对的参考点。这实现了规模效率的提高,因为信息全局分布提供额外的安全网。

[0180] 在客户端LAN外部和在云中捕获恶意流量可保护客户端的最后一英里互联网连接性免于被不期望流量饱和。将流量卸载至可缩放CFW还向客户端提供众多优点。

[0181] 本地FW15442可为独立设备、在EPD15100内部运行的软件应用(APP) 或者其他类型的FW设备。

[0182] FffSPI15446和FWDPI15444设备以及诸如负载平衡器、云防火墙或其他设备等相关设备可以定制或可由其他供应商提供现货，从而为客户端最佳选择组合。这些设备必须能够接收和转发流量、识别威胁和最重要的是能够传达威胁发现，并且从其他设备接收威胁概况和其他信息。

[0183] 随着威胁数据累积，可以对内容、图案、攻击矢量以及由FW收集的其他信息进行分析。此分析可提供对新的潜在威胁应用启发式分析的基础。

[0184] 这可仅由GVN的安全网络优化(SNO)服务或由通过安全隧道和通信路径这两者连接的相关设备组成的相似网络来实现。

[0185] 图16示出了作为全局虚拟网络(GVN)的一部分共同工作的三种类型的网络设备的软件架构的逻辑视图。如图所示，软件和硬件可以分布在网络设备内，并且可以跨不同的电路板、处理器、网络接口卡、存储器和记忆装置分布。

[0186] 一个所述网络设备是端点设备(EPD)100。另一所述网络设备是中央服务器(SRV_CNTRL)200，并且第三设备是接入点服务器(SRV_AP)设备300。

[0187] EPD100经由描述成通信路径的加密隧道而连接至SRV_AP300，该路径可以是经由加密隧道SYSC04连到存在点(POP)SYS406，通过通信路径 SYS06连到WANSYS400到通信路径SYSCP10到POPSYS402到通信路径SYSCP12。通过WANSYS400的路径还可通过常规未加密互联网。

[0188] 每个设备EPD100和SRV_AP300还可经由通信路径SYSCP08而连接到SRV_CNTRL设备200。

[0189] EPD100和SRV_AP300的软件架构彼此非常相似，区别在于每个设备在操作中的作用不同以及一些模块不同。

[0190] 每个设备的最低级是记忆装置(RAM)106、206、306和处理器 (CPU)102、202、302以及网络接口(NIC)108、208、308。所有这些都在硬件级上。操作系统(O/S)110、210、310可以是LINUX系统或者是诸如Debian或其他系统等同等系统。该操作系统描述包括用于路由、托管、通信和其他系统级操作软件的数据包和配置。

[0191] 操作系统110、210、310之上存在全局虚拟网络(GVN的)操作系统的系统软件层112、212、312。自定义命令、系统模块、管理器和其他组成部分均在此操作，同时还包括GVN的其他组件。GVN中的每种类型的设备可以具有系统软件层的这些部分中的一些或全部或不同部分，具体具体取决于它们的角色。

[0192] 数据库模块Db120、220、320和托管模块122、222和322在本示例实施例中被配置用于GVN中立API机制(NAPM)、图形用户接口(GUI) 和其他服务器侧脚本托管站点的监听、发送、处理、存储、检索以及其他相关基础级别操作。数据库120、220、320(013)模块可以是MySQL或诸如MariaDb等等效物并且托管模块122、222和322可以是Apache和PHP 脚本或其他类型托管语言。命令行脚本也使用并且可以以Bash、C、PHP、 Pearl、PythOn或其他语言编写。

[0193] 计费模块可协作并共享通过消费模型计费的信息，例如隧道流量消耗的数据量。记账模块ACC132、232、332在EPD100上操作并且SRV_AP300 具有对应计费模块。两个模块均可将向报告屏幕提供财务信息，提供支付形式、以电子邮件发送的报表和GVN产生的其他财务数据。

[0194] SRV_CNTRL200具有存储库管理器238，所述存储库管理器处理计费信息、隧道管理器信息以及可由GVN中的各种设备采用的其他数据。存储库管理器238还通过GVN的中立API机制(NAPM)来处理与连接到其他API对等体的独立设备的对等体信息、凭证和其他信息的共孚的协调。

[0195] EPD100具有API模块130，SRV_CNTRL具有API模块230并且 SRV_AP300具有API模块330。为了简单解释本示例实施例，每个设备仅描述一个API模块。实际上，根据设备在GVN中的功能，设备可以起到组合的客户端和服务器作用。

[0196] SRV_CNTRL200上的高速缓存管理器管理跨GVN的许多设备分布的多个链式高速缓存的主索引。EPD100上的压缩引擎136和SRV_AP300 上的压缩引擎336管理储存在文件上、DB表中的数据的压缩和解压，或者用于流式传输数据。

[0197] EPD100上的高级智能路由(ASR)150模块处理从EPD100经由GVN 的路由至目的地最佳出口点的流量路由。

[0198] SRV_AP300上的远程取回器BOT311是地理目的地机制(Geo_D)的核心组件。

[0199] SRV_CNTRL200上的DNS管理器254管理主DNS索引，所述主DNS 索引可以将DNS服务器播种在各种GVN设备上，诸如将DNS154播种在 EPD100上。

[0200] SRV_CNTRL200上的日志记录管理器管理本地日志记录和经由API 调用由设备共享至存储库的日志记录。本示例实施例中的日志记录管理器被赋予记录操作事件、API行为和事务的功能，并且该日志记录器还具有用于GVN操作的多个方面的其他作用和进程。

[0201] EPD100上的本地高速缓存152和SRV_AP300上的本地高速缓存352 将数据进行本地高速缓存。

[0202] GVN管理器272在SRV_CNTRL200上操作以控制在 SRV_CNTRL200和GVN的其他设备上的系统的各个组件的操作。

[0203] EPD100上的本地DNS服务器和高速缓存154以及SRV_AP300上的高速缓存354允许高速缓存DNS查找，以实现快速本地检索。DNS154 和354可以完全清洗、清除个别项，或者设定在一定时间之后删除所检索的查找的超时。

[0204] EPD100上设有内容传递代理(CDA)158，该内容传递代理是Geo-D 的组件。SRV_AP300上设有内容拉取代理(ContentPullingAgent，CPA)358，该内容拉取代理也是Geo_D的组件。CPA358与SRV_300上的BOT311一起工作，以使用从该区域播种的本地DNS354从远程区域拉取内容。 CPA358采用隧道、高速缓存和GVN的其他改进功能将抓取的内容发送到CDA158o

[0205] EPD100上、SRV_CNTRL200上和SRV_AP300上的防火墙(FW)(未示出)进行操作以保护对设备以及设备与其他者之间的通信路径的接入。

[0206] EPD100上和SRV_AP300上的连接性管理器(未图示)管理设备之间的隧道以及其他设备到设备通信路径。SRV_CNTRL200的215上的压缩管理器管理本地压缩并且还与EPD100上的压缩引擎136、SRV_AP300的压缩引擎336和GVN的其他设备上的压缩引擎协作。EH)上的

路由与 ASR150、Geo-D和其他元件协作以管理流量路由。

[0207] SDB100、SDB200和SDB300中的数据库表的结构对于设备操作来说是等效的，而每个数据库表的数据是特定于设备类型的，并且每个设备具有标识特定设备。在SRV_CNTRL200上，存储库数据库SDB202用于存储所有设备的唯一信息，并且存储库管理库238可以使用此信息来将API 凭证、隧道信息或其他信息传达给设备。

[0208] 每个设备中均存储有关于设备本身及设备的对等体对合作伙伴的标识和API对等体信息，事务列表和队列数据以及其他信息。除了所描述的用途之外，所述方法和数据库还有其他用途，但是为了简单说明，此示例仅涵盖几个示例性核心功能元件。

[0209] 拓扑

[0210] 图17示出了使用具有主干段和八角形路由的轴辐式(hub andspoke)拓扑的GVN。图17示出了两个不同区域17-RGN-A和17-RGN-B中的GVN 的网络拓扑以及所述区域如何经由路径17-POA和17-POB通过全局连接 17-RGN-ALL连接。此外，图17示出了这两个区域中的每个区域中的轴辐式连接。图17与图15相似并且以轴辐式模型的附加辐条的形式在每个区域中添加了多个出入点(EIP)。

[0211] SRV_BBX17-280和SRV_BBX17-282是主干交换服务器并且提供全局连接。SRV_BBX可能是在某个区域中用作全局链路的一个或多个负载平衡服务器。在17-17-RGN-A中的接入点服务器(SRV_AP)17-302、17-304 和17-306连接至SRV_BBX17-280。中央控制服务器(SRV_CNTRL)17-200 为该区域中的所有设备服务，并且它可能是一个或多个多主SRV_CNTRL 服务器。端点设备(EPD)17-100至17-110将通过一个或多个多个并行隧道与一个或多个多个SRV_AP服务器连接。

[0212] 此图还示出了每个区域中作为轴辐式(hubandspoke)模型的附加辐条的多个出入点(EIP)17-EIP420、17-EIP400、17-EIP430和17-EIP410，这些出入点具有通向和来自开放互联网的路径。此拓扑可通过GVN提供与远程区域中的EIP的EPD连接。在替代方案中，此拓扑也支持EH)连接到相同区域中的EIP、连接到相同区域中的EPD，或者连接到远程区域中的EPD。这些连接通过GVN安全优化。

[0213] 图18示出了在北美、欧洲和亚洲的一些GVN全局节点与其对应服务区之间的主干连接。如图18右下方的图例框所述，本文从联网视角指出的每一区被描述为全局节点。全局节点经由高性能网络链路彼此连接。各点之间的延迟时间越低，信息传输越快。

[0214] 全局节点周围的两个环表示例如从源信息所在的中心起的半径内的连接性质量区类型。这仅出于简单说明目的，因为这些区的大小和形状由许多因素决定。然而，这两个区可彼此区分成最近的区是高性能区，而另一区是最佳服务区。

[0215] 查询客户端或服务器或其他类型设备相距全局节点越远，信息流动所花费的时间越长，并且在某点处由于距离过大以致QoS下降，使得设备不再在高性能区中，而现在位于最佳服务区中。

[0216] 如果QoS降至特定阈值以下，那么设备位于最佳服务区之外，并且因此该设备与全局节点之间距离过大以致除安全外，由GVN提供的优点可能存在不确定性。

[0217] 图18示出了美国加利福尼亚州圣何塞市的区SJC18-01、美国纽约州纽约市的区JFK18-02、荷兰阿姆斯特丹市的区AMS18-11、日本东京的区 NRT18_21和中国香港特别行政区的区HKG18-22。世界范围内的许多其他地点均需要放置重要全局节点，但为了简便说明，

仅出于说明目的而示出几个位置。

[0218] 图18还示出了各个全局节点之间的代表路径，例如JFK18-02与 AMS18-11之间。实际上，两点之间存在表示海底线缆的许多路径。

[0219] 图19示出了GVN内的各个设备之间的连接性，其中指出了从辐条中的设备至中心设备的多个连接路径。SRV_BBX(主干交换服务器)19-800 和19-810点的放置点基于客户端关于相对于管道、互连的最佳互联网数据中心(IDC)的位置，用于服务于目标区域、同时经由路径19-BB2和 19-BB6连接全局位置。

[0220] SRV_BBX用作它所服务的区域的中心。中心通过在互联网中的以太网链路的顶部之上(OTT)的隧道、直接以太网链路之上的隧道、光纤之上的无限宽带、以太网之上的无限宽带或者区域之间的其他形式的连接性来彼此连接。每个中心为多个SRV_AP服务器提供服务，例如为全局区域内的一个区域提供服务的19-302、19-306、19-308。31^_4?19-312、19-316 和19-318可以为全局区域的另一区域服务。

[0221] 诸如19-100至19-128等端点设备(EPD)将与相对于它们的位置、网络连接性、对等和其他相关因素而言最适当的SRV_AP服务器连接。这些因素不断改变，并且因此连到多个SRV_AP服务器的多个隧道始终由Ero 维持。每个Ero同时与各种(一个或多个)SRV_AP服务器连接。

[0222] EPD处、SRV_AP处和其他位置处设有出入点(EIP)，该这些出入点处，流量可离开GVN进入互联网或者从互联网进入GVN，并且GVN尽可能远地保护和优化流量。

[0223] 诸如SRV_AP19-308和SRV_AP19-318等SRV_AP设备还通过19P60 等隧道路径彼此连接，以便诸如EPD19-110等两个EPD可经由路径19P22 至19P60至19P58与EPD19-128连接。

[0224] 中央控制服务器(SRV_CNTRL)19-200链接到多个设备，例如经由路径19P62链接到SRV_AP19-302，用于中立API机制(NAPIM)信息交换。 EPD还经由NAPM路径与SRV_CNTRL19-200连接。为使本示例实施例相对简单，未示出NAPJ顶EH)至SRV_CNTRL路径。

[0225] 在SRV_CNTRL与各种设备之间交换的NAPM信息可以用于共享使用统计、隧道建立信息，例如IP地址、端口、协议、安全凭证、证书、密钥，并且共享其他信息，从而实现GVN的自动和安全操作。

[0226] 图20示出了GVN模块和设备的交互方式。全局虚拟网络(GVN)由独立操作以及与其他设备协作的各种设备组成。尽管每者作用基于它们的类型和基础功能而可能不同，但是它们遵循相似的代码库、数据库模式和其他架构元素。

[0227] 基础设施安装在某个区域中，以便支持EPD和PEPD的操作。诸如端点设备(EPD)100、便携式端点设备(PEPD)和端点中心(EPH)等设备经由连到接入点服务器(SRV_AP)300的隧道将各种LAN、PAN和其他网络连接至GVN。每个设备具有自己的本地托管数据库。

[0228] 冗余是由具有多个主SRV_CNTRL和其他服务器类型的每个区域中有每种类型的多个服务器提供。中央数据存储库位于中央控制服务器 (SRV_CNTRL)200上。SRV_CNTRL的工作是经由GVN的中立API机制而连接至各种设备。经由GVN的NAP顶的API调用经由用于设备之间通信，例如EPD100到SRV_BC20-502通信的路径SOPC^JRVJ^NTRL上的Db存储库中的设备_10和注册/区域映射允许API对等体对关系管理，生成适当服务器可用性列表(SAL)并且接受日志记录。这样可实现对与SRV_AP和GW服务器的关系和连接进行有效管理。

[0229] GVN的后端服务器和基础设施设备包括反向信道服务器 (SRV_BC)20-502;安全引

导服务器(SRV_SB)20-504;认证、授权、记账服务器(SRV_AAA)20-508和日志记录服务器(SRV_LOG)20-516等等。

[0230] 网关服务器和其他设备经由连接器20AD0而连接至SRV_CNTRL200 并且经由“所有设备”中心20AD2而连接至网关设备。这可包括网关电子邮件服务器(SRV_GW_Mail)20-510、用于财务事务的网关服务器 (SRV_GW_FIN)20-518和/或作为一类其他SRV_GW_*20-512的用于第三方连接(SRV_GW_TPC)的网关服务器。

[0231] 起特殊作用的网关服务器可以针对该功能作用而调整并且以为其提供保护的方式。通过授权电子邮件网关服务器,可将其设为安全电子邮件发送器和接收器。这将需要配置和维护并且观察其操作。不过同时,无需其他服务器来处理电子邮件,从而释放那些设备的管理负担。所有设备可经由由请求发送电子邮件的动作调用发送至API的数据有效负载来转发电子邮件。有效负载中的旗标可以指示电子邮件是立即发送还是在特定时间发送,或者应当以什么优先级发送。其他设置可以管控它的发送方式。SRV_GW_EMAIL将会接收这些数据有效负载、将其添加至其电子邮件发送队列,并且电子邮件管理器将会处理传递电子邮件的时间和方式并且将相应地对该事件进行日志记录。弹回、答复和其他输入电子邮件还可以由一个点服务器类型SRV_GW_EMAIL处理。

[0232] 日志记录服务器和其他设备还可以由GVN设备经由20AD4访问。

[0233] 图21示出了关于GVN模块和设备之间的交互方式的额外细节。这些额外细节包括通信路径,例如从SRV_BC4-502至31^_0阶此200的21Q00,用于从反向信道服务器向中央控制服务器进行信息的报告。重点在于尽管 GVN设备将会需要关于其自身、其对等体、其连接性选项的信息以及其他信息来进行操作,但是将性能和其他数据共享至SRV_CNTRL200和/或其他设备可以整体地了解较大系统。恒定反馈环路允许自动调节和在传输过程中学习,以便做出更好决策。

[0234] 图22示出了GVN模块和设备的拓扑和连接性以及它们如何在互联网上与其他设备交互。图22所示通信路径包括外部路径(PE)、隧道路径(用于流量)(PT)、控制路径(CP)、加密系统路径(ES)和GVN设备之间的API 通信路径(PA)以及更多通信路径。

[0235] 中央服务器(SRV_CNTRL)200包括保存重要系统信息的文件存储库和数据库。SRV_CNTRL能够经由PA路径与所有GVN设备连接以进行API通信。端点设备(EPD)100是局域网(LAN)和互联网之间、经由各种并行潜在通信路径的网络接入点。

[0236] EPD内的高级智能路径(ASR)可将本地流量经由路径22-PE00到存在点(POP)22-020到22-PE02,发送至最靠近的互联网22-010。反向信道服务器(SRV_BC)22-502经由从22ES04通过22-010经由22ES02至201至 22ES020进入EPD100中的反向信道连接来连接至EPD100JS抽路径是加密控制路径并独立于传输流量的隧道路径。

[0237] EPD100维持连到多个接入点服务器(SRV_AP)中的每一者的多个隧道,即经由22PT00和22PT02至SRV_AP300、经由22PT04和22PT08至SRV_AP22-302、经由22PT10和22PT12至SRV_AP22-306以及经由 22PT14和22PT16至SRV_AP22-308。

[0238] 该图未按比例绘制,但是例如SRV_AP22-302和SRV_AP300在相同区域中,并且经由路径22PE04至POP22-022至22PE08至互联网22-012 以及路径22PE16经POP22-026至22PE12至互联网22-012,从GVN离开进入互联网22-012<^TM都可以对域名服务(DNS)服务器22-402进行本地DNS查找。

[0239] SRV_AP22-302和SRV_AP300这两者均维持分别经由22PA02和 22PA08至SRV_CNTRL200的API通信路径。

[0240] 网关设备(SRV_GW)22-514位于与SRV_AP22-302和SRV_AP300相同的区域中。这可发送电子邮件、处理财务事务和GVN的SRV_GW设备的其他功能性。

[0241] SRV_AP22-306经由22PA10连接至SRV_CNTRL200,并且在其区域中通向互联网22-014的出口点是经由22PE20至POP22-024至22PE22至互联网22-014。

[0242] SRV_GW服务器22-516经由22PA24而连接至SRV_CNTRL200,并且经由22PE26至POP22-024至22PE22至互联网22-014连接至互联网 22-014。

[0243] SRV_AP22-304经由22PA18连接至SRV_CNTRL200,且在其区域中通向互联网22-016的出口点是经由22PE26至POP22-028至22PA30至互联网22-016。

[0244] SRVGW22-512经由22PA14而连接至SRV_CNTRL并且经由22PA16 而连接至SRV_AP。来自SRV_GW22-516的本地流量经由22PE28而离开至POP22-208至22PA30至互联网22-016。

[0245] 在GVN内存在其他设备,并且它们承担特定作用,诸如备份服务器 SRV_Backup22-522和日志记录服务器SRV_Logging22-516。这些分别经由22PA20和22PA22而连接至SRV_CNTRL。它们可以接受从 SRV_CNTRL200或从其他设备经由PA##路径而中继到SRV_Backup522 或SRV_Logging22-516的数据。

[0246] GVN的所描述的拓扑允许来自EPD100的流量具有通过多个隧道至多个SRV_AP服务器的每区域流量的多个选项。其他设备确保信息被分布到各个设备以供有效利用。

[0247] 图23示出了在端点设备(EPD)100、23_102、23_158与接入点服务器 (SRV_AP)300、302之间的多个隧道连接性。这些隧道可以用于客户端数据流量、内部系统数据或其他传输。此图进一步说明了诸如中央服务器 (SRV_CNTRL)200和反向信道管理服务器(SRV_BC)23-502等全局虚拟网络(GVN)基础设施设备与GVN中的其他设备的连接。

[0248] SRV_BC23-502建立并且维持至反向信道隧道23PA02至EPD100、23P018至EPD102、23PA06至EPD23_158、23TP50至SRV_AP23-302等等。GVN内可能存在更多SRV_BC服务器,以便一个SRV_BC不操作的情况下提供冗余,并且还通过将SRV_BC服务器置于靠近它们连接到的设备的策略位置来确保最佳性能。

[0249] EPD100将一个LAN23-002连接至通过GVN的数据所采用的各种路径,诸如经由三个多个隧道23TP00、23TP02或23TP04中的一者至 SRV_AP300、经由路径23PE00至出口点至互联网23-410。

[0250] 另一路径是经由三个多个隧道23TP10、23TP12或23TP14中的一者从SRV_AP300至SRV_AP23-302。

[0251] 从SRV_AP23-302的路径选项是经由23-382至互联网23-412出口点。

[0252] 从互联网23-412进入GVN的外部入口点X-IP305允许由非GVN设备连接以通过GVN对设备进行寻址和访问,从而实现在由GVN传输的流量通行的持续期间内增强GVN。

[0253] 由GVN实现的另一益处是与提供与在云中的服务提供合作伙伴组织的位置处的EPD23-158的安全隧道连接,以便实现经由GVN通向它们的服务器和在LAN23-152的位置处的相关服务的安全隧道。

[0254] 从LAN 23-002至LAN23-012的LAN-WAN-LAN网桥可以经由从 23-002至23CP02至GWD23-004至23CP04至EPD100至 23TP0023TP0223TP04至SRV_AP300至23TP1023TP1223TP14

至 SRV_AP23-302至23TP2023TP2223TP24至EPD23-102至23CP14至 GWD23-014至23CP12至LAN23-012的通信路径。由这个网桥传输的所有流量由GVN机制提供保护并且改进。

[0255] 在两个设备之间的多个隧道诸如23TP0023TP0223TP04或 23TP1023TP1223TP14或23TP2023TP2223Tp24可通过沿着一个隧道发送流量而提供单个通信路径,或者两个或更多个隧道可聚集在一起,其中两个或更多个绑定隧道可如同是一个隧道那样传输流量。

[0256] 具有在对等体对之间的API通信路径以及连到其他设备的隧道的 SRV_CNTRL 200可以用于经由路径例如23PA00至EPD100或23TP30 至23-302至23TP22至EPD23-102或23PA04至23-302至23TP60至 EPD23-158和其他潜在选项进行文件传输和数据交换。

[0257] 在本示例实施例中存在其他可能通信路径,并且还存在通过GVN的通信路径的更多选项。在本示例实施例中,所有隧道都表示了经由GVN 的第三层的链路,它们各自构建在互联网之上的GVN第一层上。

[0258] 图24是当今互联网的工作原理的简化示例图,其中考虑到跳跃计数或生存时间(TTL)以及由于对等关系和相关路由政策采取的路径。

[0259] A0表示互联网服务供应商(ISP)的网络。A1至A06表示存在点(POP),并且这些POP进一步连接至交换机设备或客户端设备以便将它们链接至互联网。此跳跃和轴辐式结构示出更广的ISP网络内的网络群集。具有线帽形式的圆圈的线指示此连接性。为了简单起见,在本示例实施例中,A1、A2、A3和其他POP的结构没有示出最后一英里网络的链路,但是应当暗指这些链路。每个POP具有其自身至网络的轴辐式连接性,诸如局域网 (LAN)或经由POP实现互联网连接的互联网数据中心(IDC)。

[0260] H0是单宿主ISP的示例,表明它依赖于其与互联网之间的一个路径。如果此路径被切断或发生故障,那么从此ISP至更广互联网的连接性就被切断。

[0261] B0是它本身与其他ISP网络之间示出了五个连接的多宿主ISP的示例,即使一个路径不可用,流量仍可流过互联网,但是是通过不太直接路径进行的。

[0262] 1X1和1X2是互联网交换(IX)的示例,互联网交换可能通过主干或主干专用连接彼此独立链接。IX是ISP和其他ISP可以在“与我会和房间 (meet-meroom)”处或用于直接网络至网络对等连接的等效布置中彼此连接。

[0263] ISP的网络与其他ISP的网络之间也存在通信路径,或者它们之间存在IX或与中间路由器。这些主干通信路径由在两端有箭头帽的线示出。中间设备由带箭头帽的线之间的圆圈示出。IX之间的回程连接性由两端有箭头帽的虚线示出。分页连接符IBH1用于示出国际回程(IBH),即1X2 还具有与未在本示例实施例中示出的另一IX的连接性。

[0264] 为了示出在ISP之间的直接有效连接,从A0至G0经由路径AX1-1->AX1-2_>IX1->GX1-1仅有四个中间跳跃并且应是最有效的路由。

[0265] 为了示出因路径故障导致的迂回路径,如果路径GX1-1发生故障,那么来自H0或A0的以G0为目的地的流量将无法经由1X1通过GX1-1。替代选择是流量经由B0和E0去往G0。过去从A0经由AX1-1-〉AX1-2-〉 IX1-〉GX1-1只需4个中间跳跃,现在需要更多跳跃AX1-1至AX1-2至 1X1至BX1-4至BX1-3至BX1-2至BX1-1至B0至EB-5至EB-4至EB-3 至EB-2至EB-1至E0至GE-3至GE-2至Ge-1才能G0。如果GX101发生故障,那么现在从A0到达G0的流量需要17个中间跳跃和对应的较高延迟时间。

[0266] 同时,应经过GX1-1的单个中间跳跃的从G0至1X1的流量将不得不从G0去往E0至B0

并随后到达1X1。

[0267] 此额外流量可能耗尽连接，并且可能造成较高延迟时间和与拥塞相关的分组丢失。通过IX对等通常将会具有多得多的容量和能力来处理大体积的流量。当从G0至1X1的单个中间跳跃GX1-1不可用时，通过替代路由的额外跳跃(TTL)和往返时延(RTT)可能导致跳跃过多或者时间过长，继而导致分组被标记为不可传递或基于互联网的服务超时。

[0268] 两个ISP网络之间经由IX和通过采用回程实现的最佳连接性由路径H2至H0至HX1-1至HX1-2至1X1至X1X2-1至X1X2-2至IX-2至DX2-2 至DX2-1至D0至D2表示。这样，从POP至POP共12个跳跃。

[0269] 下一直接路径应是经由B0，共16个跳跃。路径是H2至H0至HX1-1 至HX1-2至1X1至BX1-4至BX1-3至BX1-2至BX1-1至B0至DB-4至 DB-3至DB-2至DB-1至D0至D2。

[0270] 下一直接路径将是经由A0经由C0，共19个跳跃。路径是H2至H0 至HX1-1至HX1-2至IH至AH-2至AH-1至A0至AC-1至AC-2至AC-3 至AC-4至AC-5至C0至CD-1至CD-2至CD-3至D0至D2。

[0271] 由于路由政策和对等关系，间接但可能的路径可以是30个跳跃，例如经由G9经由E0经由B0经由F0。路径是H2至H0至HX1-1至HX1-2 至1X1至GX1-1至G0至GE-1至GE-2至GE-3至E0至EB-1至EB-2至 EB-3至EB-4至EB-5至B0至FB-5至FB-4至FB-3至FB-2至FB-1至 R)至DF-5至DF-4至DF-3至DF-2至DF-1至D0至D2。

[0272] 当流量无法到达目的地时就会发生循环，这是因为不良或不正确的路由政策管控起始地和目的地之间的中间设备而造成的。例如，如果来自 C0的流量期望路由至G0，那么由于C0可能认为B0和E0彼此靠近并且这是最佳路径，因此C0在认为B0将向E0发送流量时就会选择去往B0。然而，B0可能不直接与E0对等，而与F0具有强对等关系。F0也不具有对等关系或到达E0的路径，并且因此其可能将流量发送至D(LD0仅具有将流量发送至C0或至B0的两个选择，在两种情况下，最终结果都是流量循环、不可传递。这种循环还有其他原因，诸如路由表故障、设备受损、入侵和其他错误行为或者其他原因。

[0273] 过多跳跃和过高延迟时间的最终结果是超时或分组被丢弃。

[0274] 图25示出了用以增强性能的基础设施的策略定位。在这个示例内存在三个或四个关键点，其中SRV_AP服务器和其他GVN基础设施的策略定位将会确保在所示出的示例网络拓扑上的所有点之间的最佳对等和性能。

[0275] 为了包括可选路由选项和故障恢复而在IX1_IDC、B5和IX2-IDC处以及有可能在D5处，安装和操作的SRV_AP服务器将会提供与其他所有网络的对等并且通过提供绕过任何损坏路径进行路由的选择而提供 SRV_AP之间的稳定路径。这种策略定位提供实现其他性能增强的灵活性和可能性。

[0276] 图26示出了GVN可如何结合诸如网络弹射(NetworkSlingshot)等技术以跨距离无缝地实现很多优点。网络弹射(NetworkSlingshot)进一步在美国临时专利US62/266,060中描述。

[0277] 第一边界是互联网和GVN之间的GVNEIP26-322。下一边界是安全周界26-182。这种分层安全方法保护GVN所立足的核心基础设施。

[0278] 在GVN与GVN主干之间的安全周界26-182保护高速全局网络。在周界26-822之上的GVN部分具有经由安全GVN隧道在开放互联网顶部之上(OTT)流动的流量。在安全周界26-

182下,GVN连接采用在暗色光纤之上的各种协议或不可从互联网直接到达的其他连接。

[0279] 超级计算机节点26-538可在安全周界26-832内部(下方)操作,所述安全周界可操作具有高级特征例如对平行文件系统(PFS)26-602设备的远程直接记忆装置存取(RDMA)的真实内部网络。

[0280] 图27示出了在各种GVN设备的数据库上的表如何彼此相关和它们交互方式。例如,SRV_CNTRL上的存储库数据库DB_2300上具有关于设备以及设备之间经由GVN的中立API机制(NAPIM)的交互的各种表。数据库DB_2300中的表例如设备注册表DBT_2310被指定为REPO_ACTIVE,这意味着该表从许多来源接收信息,进行读取/写入并且能够作为信息源被查询以用于选择性地或完全地将表例如设备标识 DBT_2102复制作为数据库EH)本地DbDB_2100的一部分。此表DBT_2101具有标识SEL_REP+W,这允许从DBT_2310选择性地复制并允许将相关标识回报给设备注册表。

[0281] 信息的控制和释放由数据管理器管控。数据库表类型指示符包括正常读取/写入表“常规”(RE⑶LAR)、只读复制表REP_INFO、仅具有相关行的只读部分复制表SEL_REPSEL_REP、从诸如标识等设备注册表 DBT_2310的存储库上的所有源的合并表REPOS_ACTIVE。其他的可能性包括来自要在SRV_LOGS上的数据库DB2800上合并的源表的“日志记录”(LOGGING)。表的这些标识仅是用于举例目的并且可在现实用途方面不同,并且基于用途存在更多的表和其他类型。

[0282] 图28示出了在各个模块、机制、技术和GVN其他组件之间的协作成果。

[0283] GVN存在3层,层1是在其顶部之上(OTT)建立GVN的物理网络层,例如互联网。层3是被客户端设备视为通向目的地的部分或完整路径的 GVN网络层。层2是这二者之间的逻辑层。

[0284] 存在与物理条件28-00交互的组件。28-20处的动态构造模块致力于维持GVN的连接性。本文所述的联合作用部分将GVN的相关模块链接至物理28-00和动态28-20元件。例如,为了使高级智能路径(ASR)模块 G106适当运作,必须将多个接入点服务器(SRV_AP)GP106置于具有路由和对等GR106的多个位置。为了使EPD能够选择最适当的SRV_AP以与之建立连接,需要关于哪个SRV_AP最佳的信息。ASR服务器可用性模块SA106基于由ASR测试管理器TM106提供的信息为该特定EPD对服务器进行排名并且当EPD需要建立新的隧道时,它会采用服务器可用性列表SA106来建立新的隧道。随后,经由TM106在所述隧道上运行测试。

[0285] 作为另一示例,为了操作NAPIMG102,主机服务器上需要API监听器和处理器HL102AAPIM中的主机客户端和主机服务器这两者上均运行操作管理器OM102,以处理API请求和响应的准备,然后发送、处置、处理。NAPIM的动态构造需要对等体管理PM102、相关NAP顶动作管理 AM102以及在物理TP102和动态TM102处的事务。

[0286] 构造

[0287] 图29示出了GVN的高级智能路由(ASR)特征。具体来说,该图示出了对通往世界多个区域中的出口点的多个路径的端点设备(EPD)103内的GVN的高级智能路由(ASR)特征。

[0288] 在本示例实施例中的流量从诸如主机客户端101等已连接的设备在LANA102中开始。在本示例实施例中示出的目标流量区域是:1)本地流量经由POP401停留在本地,其中GVN隧道将不一定会使性能提高;2) 本地流量在加密隧道TUN1中载送到互联网203;3)送往另一区域的流量经由TUN2到达该区域中的SRV_AP301以访问互联网303;以及4)流量经由

TUN3到达其他远程区域,其中在SRV_AP501上存在一些ASR。

[0289] EPD103内的DNS高速缓存103-4从每个目标区域处的DNS服务器进行DNS查找,包括用于互联网402的DNS404、用于互联网203的 DNS204以及用于互联网303的DNS304以及用于互联网503的DNS504。内部DNS高速缓存103-4能够经由路径DP4进行访问。

[0290] EPD103的物理网络接口控制器(NIC)硬件设备包括四个端口。ETH0103-9是经由通向ISP的通往互联网402的POP401的P401将 EPD103连接到互联网的网络接入点(NAP)的WAN端口。来自EH)的所有流量都会经过作为GVN网络的第一层的该连接。在这个连接之上的TUN 隧道是GVN的第三层。ETH1103-1是经由路径P102连接到LANA102的局域网(LAN)端口。ETH2103-2是经由路径P104连接到LANB104的另一物理LAN端口。最后,存在充当网桥BR0103-3的虚拟接口(VIF),用于分别经由内部路径DPI和DP2连通LAN接口103-1和103-2。

[0291] 来自LAN网桥BR0103-3的流量经由设备路径DP3发送到虚拟接口 (VIF)链。在每个VIF处应用高级智能路由(ASR),利用IP地址的路由表在将流量流从每个VIF引向两个或更多个出口点中的一个。最后一个 VIF对“所有其他”剩余流量可能只有一个可能的出口点。

[0292] 例如,在VIF0103-5处,本地流量经由P401离开。通过VIF0103-5 的所有其他流量经由DP5发送到所述链中的下一个VIF,即,VIF1103-6。来自VIF1103-6、目的地为互联网203的流量经由路径P201从EPD103离开,通过加密隧道TUN1到达SRV_AP201,然后到达路径P202到POP202 到P203再到互联网203。从此位置,可经由路径P204通过SRV_DNS204 来查询区域DNS查找。可分别经由P205和P206连接到主机客户端205 或主机服务器206。

[0293] 来自VIF1103-6的任何剩余流量经由路径DP6发送到VIF2103_7。基于应用到VIF2103-7的路由表,目的地为互联网303以及该位置处的相连设备例如主机服务器306的所有流量经由路径P301离开VIF2到达TUN2 到SRV_AP301,并且继续通过互联网303并且到达互联网以外的其他地方。

[0294] 来自VIF2103-7的任何另外剩余流量将发送到VIF3103-8。来自VIF3103-8的所有流量经由加密隧道TUN3发送到SRV_AP501。在 SRV_AP501处应用ASR路由,使目的地为互联网503内的IP地址的流量经由路径P502发送POP502再到到互联网503。

[0295] 来自SRV_AP501、目的地为互联网603的流量经由相连的加密隧道 TUN4发送到SRV_AP601到路径P602到POP602到P603再到互联网603,并且到达互联网以外的其他地方。

[0296] 可对SRV_DNS604进行互联网603的区域中的DNS查找,并且可例如经由通向主机服务器605或其他设备的P605连接到该位置处的设备。

[0297] 这种ASR机制可以在各种流量结点处使用,以便优化地将流量发送到位于多个目标区域中的互联网上的最佳出口点流量,从而实现地理目的地流量,并且获得由GVN实现的其他优点。

[0298] 图30示出了在客户端(C)与服务器(3)之间建立一系列加密隧道。步骤30-0至30-18示出了在C和S之间的一系列的简化通信。

[0299] 第一步骤是打开从C到S的连接30-0。下一步骤是S接受连接握手 30-2。如果握手数据格式有误或者与预期格式不符,那么过程可在此停止。

[0300] 接收和接受握手30-4后,C向S提供证书,以便S将该证书连同所需安全信息一起用以在这两者间建立安全套接字层(SSL)连接30-8。将从 C接收的证书与S上的对应证书密钥进行比较。如果证书过期或不正确,那么就将无法建立SSL连接,并且过程将停止。

[0301] 这种连接将被用于从C向S发送关于隧道的信息30-10,包括通行短语、量度和关于隧道量度的其他信息,包括每个设备将使用哪个IP地址和端口来进行隧道流量,以及其他信息。

[0302] S将针对其自身版本的隧道量度和通行短语以及其他信息来验证这个信息30-12。如果信息并不准确,那么过程将在这个步骤停止。

[0303] 在成功验证后,S将向C发回响应,使得C可以利用所提供的配置设置开始发起或构建隧道的过程30-14。

[0304] 在隧道建立后,可以在C或S或这两者处应用路由30-16。虽然已建立了隧道,但是在向其添加路由的过程期间,流量可能无法流过隧道,或者即使流量能够流过隧道,也会存在数据泄漏风险。这种风险发生的原因是,应用所有路由之前,送往目标IP地址的流量可以在不加密或行进通过隧道的情况下离开默认出口路径到达互联网。已将路由添加到隧道后,后续流量将受保护,因为它将被传输通过隧道。根据要对隧道应用的路由表的大小,这个延迟可能是相当长的时间量。

[0305] 当路由全部已全部应用到隧道时,隧道可用于将流量推送通过其中30-18。

[0306] 图31示出了对等体对中的两个对等体所需的信息流。所述对等体可以是客户端(C)与服务器(S),或者P-2-P拓扑中一个对等体到另一个对等体。为了简化本示例实施例中的标记和描述,C至S和P-2-P表示相同类型的两个对等体关系,本文中描述的是C到S关系。GVN主要使用设备之间的C到S关系,但是其方法和技术也可以应用于P-2-P对等体对用于进行隧道构建。

[0307] 加密隧道在本质上是数据可流过的安全通信路径。当客户端和服务器隔开一定距离并且它们之间的连接是在开放未加密的互联网之上时,加密隧道是用来安全交换数据的理想通道。如果任一端均有人类网络管理员,那么他们就可以对设备进行编程。不过,关于如何中继如通行短语、密钥和其他信息的安全信息存在挑战。有些可以使用语音电话进行协调,有些可以通过安全网站使用一系列的帖子共享信息,或者可以使用其他方法。可能需要执行手动设置单个隧道的任务。管理多个隧道可能变得麻烦。

[0308] 为了在对等体对中的两个设备之间自动构建一系列的加密隧道,需要安全地共享信息。隧道信息还需要是当前的并安全储存在设备上。此外,在建立过程期间,存在必须要解决的威胁。虽然已建立了隧道,但是存在将需要解决的其他威胁。

[0309] SRV_CNTRL31D00是中央服务器,其中包括存储库,所述储存库管理数据库表中的信息、储存在安全文件储存系统中的文件、位于储存器中的列表以及其他相关信息。SRV_CNTRL还具有评估某些数据以生成信息报告的算法和机制。

[0310] 客户端设备31D02表示将经由特定IP地址和端口通过“拨号”连接到服务器设备来发起隧道构建的设备。许多客户端32D02设备可采用类似的软件和配置同时连接到GVN,设备之间的区分性因素为唯一设备标识 UUID,以及每客户端每通道的唯一信息。

[0311] 服务器设备31D06表示将收听在特定IP地址和端口上的客户端连接尝试的设备。如果客户端遵循正确的协议和建立顺序,并且提供正确的凭证和其他安全信息,那么服务器将允许客户端构建通向服务器的隧道。许多服务器31D06设备可采用类似的软件和配置同时连接到GVN,区分性因素为唯一设备标识UUID和唯一信息。

[0312] 隧道信息31S2示出储存在客户端设备31D02和服务器设备31D06上的信息。每个设

备可以建立多个隧道,并且每个隧道将具有其自己的隧道信息和安全信息集合。一些隧道信息集合可以用于构建当前活动隧道,并且其他隧道信息集合可以保存在储库中以供用于未来隧道。

[0313] C与S之间的某些信息是等同的,例如一个将呈现给另一个的密码短语,其他信息将取决于可用性而有所不同。在两点之间构建隧道的信息要求可以包括:客户端/服务器拓扑和设置;隧道将使用的每个端点的IP和端口;隧道量度,包括MTU大小、协议和用于其操作的其他信息;密钥、通行短语和有关隧道使用的安全保护的其他信息;SSL证书以及用于保护隧道建立前的信息交换的其他信息;以及其他信息。这些信息使用GVN的中立API的特定API动作调用在设备之间共享。

[0314] 隧道前31S0描述在设备31D0231D06与SRV_CNTRL上的存储库 31D00之间接收和共享信息,并将其返回到设备31D0231D06的过程。API 通信路径API-31CP0、API-31CP2、API-31CP4和API-31CP6表示请求- 响应信息交换,箭头表示从一个设备到另一设备的信息流动方向。

[0315] 服务器31D06经由路径API-31CP0将信息报告给SRV_CNTRL31D00 设备的接收信息31C-0模块。SRV_CNTRL31D00从服务器接收信息,并且将相关标识、隧道、当前负载和其他信息储存在其存储库中。例如, SRV_CNTRL31D00上的算法和AI逻辑分析服务器负载,并且基于来自客户端31D02设备的当前需求和预期需求,对服务器可用性C-1矩阵进行更新。服务器可用性C-1信息可以通过以下方式传输:共享信息31C-6模块通过GVN的API经由API调用路径API-31CP6将数据库复制到客户端 31D02;经由GVN的直接文件共享;或者其他方法。

[0316] 客户端31D02经由路径API-31CP2将信息报告给SRV_CNTRL31D00 设备的接收信息31C-0模块。这个信息将会储存在SRV_CNTRL31D00的存储库中。来自客户端31D02的特定隧道信息可由共享信息31C-6模块经由路gAPI-31CP4与服务器31D04共享。

[0317] SRV_CNTRL31D00编译每服务器的当前客户端31C-4列表,该列表经由共享信息31C-6模块、经由路径API-31CP4发布到服务器31D06。

[0318] 如果客户端31D02或服务器31D06检测到利用当前隧道信息建立隧道存在问题,那么一个设备或另一设备可以分别经由API-31CP2或 API-31CP0请求由SRV_CNTRL生成新的隧道信息集合。可经由共享信息 31C-6与对等体对中的这两个对等体共享新的隧道信息集合,其中客户端 31D02信息经由API-31CP4发送,并且服务器D02信息经由API-31CP6 发送。

[0319] 所述客户端31C-4列表以及服务器31D06的当前状态将直接影响到服务器可用性31C-2。

[0320] 每个服务器31D06需要整理、保护和协调其客户端31C-4列表,客户端31C-4列表将尝试为服务器31D06的共享资源建立新的隧道。这个信息将会是流畅的,并且需要经由对SRV_CNTRL31D00的安全API调用进行定期更新。

[0321] 在设备之间安全协调信息的需要对于保护它们之间隧道的完整性是必要的。

[0322] 隧道构建31S4阶段描述经由共享信息31C-6进行隧道建立的过程。参考图30,了解在客户端与服务器之间构建隧道所采取的步骤。路径 31TP0表示在客户端31D02与信息交换31C-10之间以及从信息交换 31C-10经由路径31TP2到达服务器31D06的路径。

[0323] 建立威胁31C-8是指在隧道建立期间对信息交换31C-10的威胁。如果隧道类型的签名是可见的,那么在隧道建立期间可能存在威胁31CC-8,诸如来自中间非法操作符的伪

传输层安全性(TLS)握手、握手时的TLS错误、造成阻塞或阻碍的端口和IP标识、滤波设备引起的超时、中间ISP 或防火墙或设备发送的重置分组或其他威胁。

[0324] 如果信息交换31C-10成功,那么执行构件隧道31C-12步骤,其中将应用路由以及其他相关操作,以使得能够在客户端31D02与服务器31D06 之间安全构建隧道TUN。

[0325] 隧道建立31S6描述在通过隧道的正常流量流期间的阶段。必须要在设备之间传达信息,并且需要SRV_CNTRLD00管理各种客户端31D02和服务器31D06设备的唯一信息,以及在它们之间构建的多个隧道的唯一信息。

[0326] 在设备之间的信息交换必须定期发生,因为常常需要形成全新动态隧道。在IP地址上的一些端口可能被阻塞或变得阻塞,并且只要改变该IP 地址的端口就将允许构建隧道并使数据流动。此外,每个隧道需要每IP 地址一个或多个唯一端口,以便避免隧道之间的冲突。当客户端31D02 设备请求创建新的隧道信息时,生成随机端口号,并且针对以下两个或更多个的因素检查目标服务器31D06上的该特定IP地址的端口可用性:该端口是否已经被现有隧道使用(可操作的端口或可进入操作状态的备用端口);以及该端口过去是否曾被特定客户端31D02/服务器31D06对等体对使用过并且是否已被阻塞。在两种情况下,都将生成新随机数。每IP地址有65,536个可用端口,其中保留一定数量用于特定服务。例如5,500 的下限值将剩余60,036个可用端口,这些可用端口可由最小值为5001、最大值为65536的随机数字发生器使用。当拆除隧道并且将端口标记为对于某个对等体对阻塞时,可供其他对等体对使用。该端口释放是必要的,以便避免端口耗尽。因此,SRV_CNTRL31D00对IP和端口组合的跟踪是必要的。

[0327] 隧道可通过步骤来帮助其自己的建立,但是这也有局限性。虽然是安全的,但是大多数的隧道在建立期间是可见的。关于该隧道的类型的握手和签名都在操作期间可见。手动设置密钥繁琐并且不会经常改变,而且如果使用时间过长,就有可能增加它们被损坏风险;因此,密钥应当经常重新替代成新的密钥。

[0328] 自动系统需要确保可以创建诸如新的密钥、IP地址的端口和其他信息等信息,并且该信息可用于对等体对的两方以使得能够进行隧道的构建和重建。这两方必须被配置并准备好能够建立隧道。因此,对等体对之间的信息交换需要是安全的,否则隧道本身的安全整体性将被破坏。

[0329] 虽然隧道已经建立并且推送流量,但是存在操作威胁31C-14。隧道签名可能是可见的(例如,如果隧道是能够嗅探的而不会被混淆的话)。如果能够发现隧道类型,那么就会知道隧道结构。这造成了以下风险:分组流被夺取,并且使用强力密钥破解来将隧道内容解密。如果重置代码或其他隧道控制代码是已知的,那么重置信号可能中断隧道。因此,为了维护对等体对中的客户端31D02和服务器31D06设备之间的隧道安全性和完整性,需要自动并且安全地进行信息的更新和共享。

[0330] GVN结构使设备能够基于最近信息在对等体对之间自动安全地建立隧道。安全特征和方法的组合提供自我加强保护。

[0331] 图32-35示出了GVN的相对于GVN隧道的中立性和安全性的第三层,同时将跳跃数与基础互联网连接的跳跃数进行比较。在这些附图中使用术语LAN一般是有意的,并且可以表示家庭或办公室或互联网数据中心(IDC)的网络。设备可以是连接到LAN的客户端或服务器。图32示出了从LAN到EPD到SRV_AP到互联网的GVN隧道。图33示出了从LAN 到EH)到SRV_

AP至IjEro到LAN的GVN隧道。图34示出了从LAN到 EPD到SRV_AP到SRV_AP到EH)到LAN的GVN隧道。图35示出了图 34的从LAN到EH)到SRV_AP到SRV_AP到EH)到LAN的GVN隧道的附加元素,其包括对等点。

[0332] 所有四个附图都包括了从EH1到EH17的共同基线元素,其表示了基础互联网连接的外部跳跃。在每个跳跃之间的距离不按比例,并且并不表示除跳数之外的任何东西。其他公共元素包括在在一端处具有网关设备 GWD1的局域网LAN1和在另一端具有GWD2的另一LAN2。本示例实施例的每个变型还具有连接到接入点服务器AP-1的GVN端点设备 EPD-1。这些设备之间存在隧道,并且GVN的第三层内的每个设备NH1 和NH2都有一个中立跳跃。

[0333] 图32示出了从LAN到EPD到SRV_AP到互联网的GVN隧道。隧道还可在另一方向上起作用,从而提供从互联网到GVN隧道再返回LAN 的入口访问。在AP-1与互联网之间存在存在点POP-1。在互联网和GWD2 之间存在另一POP-2,其表示了用于该LAN的连接的网络接入点(NAP)o

[0334] 图33示出了从LAN到EPD到SRV_AP到EPD到LAN的GVN隧道。这种变型示出经由一个SRV_AP在两个LAN的边缘之间的端到端 GVN隧道。这种变型与图32之间的差异在于隧道延伸通过从EH3通过互联网到H115的整个传输。示出第二EPD-2。

[0335] 在EPD-1与AP-1之间存在一个隧道。这联接至在AP-1和EPD-2之间的第二隧道。与在H13与H115之间的基础互联网上的13个跳跃相比,在GVN的第三层内存在由NH1、NH2和NH3表示的三个中立跳跃。

[0336] 因此,从LAN1到LAN2的总跳跃计数为从LAN1到GWD1到NH1 到NH2到NH3到GWD2到LAN2最少七个跳跃。端到端计数包括在从 EH1到EH17的两端处的两个内部跳跃,并且总计最少17个跳跃。

[0337] 图34示出了从LAN到EPD到SRV_AP到SRV_AP到EPD到LAN 的GVN隧道。这种变型示出经由两个(或有可能更多个)SRV_AP在两个 LAN的边缘之间的端到端GVN隧道。这种变型与图33之间的差异在于第二AP-2被插入路径以表示隧道AP-1到AP-2和隧道AP-2到EPD-2的另一联接。添加另一内部中立跳跃使GVN的第三层内的跳跃计数达八个。

[0338] 图35示出了图34的从LAN到EPD到SRV_AP到SRV_AP到Era 到LAN的GVN隧道的附加元素,其包括对等点,该对等点将ISP与网络边缘之间的点对等。这种变型示出经由两个SRV_AP在两个LAN的边缘之间的端到端GVN隧道,并且还进一步示出关于在EH-3与EH-15之间载送流量通过互联网的某些部分的不同互联网服务提供商(ISP)更多信息。

[0339] 这种变型与图34之间的区别在于已指示了附加元素。如图9所示的以下元素在本示例实施例的这种变型中已被覆盖:a)EDGE-1是LAN-1的设备与ISP-1的POP之间的网络接入连接的分界点;b)PP-01是ISP-1与 ISP-2网络之间出现对等的点;c)PP-02是ISP-2与ISP-3网络之间出现对等的点;以及d)EDGE-2是LAN-2的设备与ISP-3的POP之间的网络接入连接的分界点。

[0340] 可通过将SRV_AP_1放在PP-1处以使这个SRV_AP直接可与ISP-1 和ISP-2两者对等来实现某些优点。可通过将SRV_AP-2放在PP-2上以使这个SRV_AP直接可与ISP-2和ISP-3两者对等来实现更多优点。如果 ISP-2的网络不太理想,那么可替代地通过另一路由或线路或ISP或载体由GVN绕开ISP-2路由流量。

[0341] 通过GVN的中立第三层的跳跃计数仍然如图34中的那样保持为八个。在ISP之间的

距离不按比例。此外，ISP的网络内可能有更多跳跃，但是为了简单起见，已经简化所示数量。

[0342] 虽然图33、图34和图35都示出了在AP跳跃处的隧道的联接，但是这被视为LAN1和LAN2内的客户端设备的单个隧道。这个单一隧道表示 GVN的中立第三层，在第三层内能够运行将通常在互联网上传输的所有流量，包括TCP、UDP和其他协议，除此之外还有其他隧道，诸如IPSeC、 OpenVPN、PPTP等等。GVN的第三层还实现了其他优点。一些优点包括较低TTL和对路由具有更多控制的能力，除此之外还有其他优点。

[0343] 图35示出了将各种网络结构一起编入网络毯式框架中。本示例实施例示出在物理层处将各种网络结构编在一起，全局虚拟网络(GVN)在物理层之上(OTT)操作。在物理层36102处的这些结构构成一系列的网络节段，这些网络节段可以例如是IPv4和IPv6感知的，或者仅是一个或另一个协议。端点设备(EPD)36100到LAN(36000)可以是IPv4和/或IPv6。隧道TUN36P2可以是EPD36100与接入点服务器(SRV_AP)36300之间的一个或另一个协议或是两个协议。

[0344] 出口/入口点(EIP)36302指示在互联网层级上从GVN到网络结构的出口点和入口点。路径36P04指示与IPv4互联网网络36400的连接，并且路径36P06指示与IPv6互联网网络36600的连接。

[0345] 关键点是GVN的毯式框架允许诸如IPv4互联网36408的结构到 LAN3600中的IPv4的端到端链接或从互联网36600到LAN36000的端到端IPv63608，即使在物理层级36102上可能存在一些不同节段也是如此。

[0346] 图37示出了GVN中的用于自动化设备协作的通信通路。本示例实施例示出了由中立API机制(NAPIM)API3720237206372O8用来实现在一起工作以构成全局虚拟网络(GVN)的各种设备之间的自动化交互的通信通路，诸如P37202-C。

[0347] 关键操作方面可自动化以便促成快速系统响应。这些包括基础架构操作、心跳例程、连接、测试和诊断、以及其他功能。

[0348] 基础架构操作诸如有可预测性地使设备操作系统软件和数据包从可靠来源更新、维护GVN模块和数据库、以及其他操作。例如，端点设备 (EPD)IOO可以沿着路径P37202-B至37202-C经由API37202查询中央控制服务器(SRV_CNTRL)200。在另一示例中，电子邮件门户服务器 (SRV_GW_Email)37310可从作为受信任的系统软件的可靠来源的 SRV_CNTRL200来更新系统数据包。

[0349] 经由守护进程或其他重复周期操作运行的其他项诸如心跳功能包括通过从设备(诸如接入点服务器(SRV_AP)300)经由API37202通过路径 P37202-A到P37202-C向SRV_CNTRL200进行报告保持服务启动、运行和健康。还存在有诸如经由API37208通过路径P37208-A到P37208-C的冗余路径。其他心跳功能可以保持队列运行和将队列清除，可以复制日志记录数据，并且可以进行其他此类操作。

[0350] 对于连接(诸如在EPD100和SRV_AP300之间的隧道P37206-C)，该隧道的两端、SPSRV_AP300处的监听器和启动器EPD100要求相关信息。这个信息可以包括与每个设备相关或与隧道相关的对等体对信息。两者都是经由经由API37202的独立路径与SRV_CNTRL200通信。

[0351] 通过将多个隧道挂接到虚拟接口以及在设备之间的多于一个隧道的选项(诸如

EPD100至SRV_AP200或SRV_AP200至SRV_AP20x之间),要求各种不同API调用管理多个隧道、路由、以及其他信息。

[0352] 功率服务器可用性算法依赖对各种信息的系统分析,以便为EPD提供它们可经由隧道连接的SRV_AP服务器列表。由于每个隧道在映射到 GVN构造的任一端部处要求IP地址和端口以便路由清晰,因此需要更新正改变的信息。自动化设备协作有助于此。

[0353] 用于信息共享的关键部件是用于来自层1物理网络、来自GVN构造层3、以及来自GVN层2处的逻辑的测试和诊断数据的信息共享。这个连接信息提供关于对SRV_CNTRL200的分析的更多信息。对这个数据的复制也可经由API37208或其他通信路径送往日志记录服务器。分析结果也可储存在日志记录服务器上。

[0354] API还可用于更新关于配对中的每一个对等体本身的信息(诸如对等体对凭据、ID、以及其他信息)、每一个对等体上的队列、用于调解的事务日志,通过内部安全审核进行更新,并且用于更新或添加或弃用API 机制本身的动作功能。

[0355] 系统和资源监测和报告对于自动传达有关服务启动和正在运行、主机正在工作、数据库引擎启动和正在运行、安全系统正在运行和更多的信息同样是关键的。

[0356] 图38示出了动态隧道建立的问题和挑战。这个示例使用了从GVN的存储库38R-00到设备38D-00的文件、数据库结构和其他数据的传输来说明动态隧道构建的问题和挑战。在大多数的情况下,存储库38R-00将是在GVN的中央服务器(SRV_CNTRL)上。设备38D-00可以是端点设备 (EPD)、接入点服务器(SRV_AP)、网关服务器(SRV_GW_XX)或GVN的其他设备。

[0357] 根据设备类型,新创建的设备可以加载要在首次引导期间配置的主盘的复制体,或者如远程服务器的情况那样,第一引导脚本将安全地传输到服务器以运行来拉动基本系统文件。其他可能情景可以结合预先加载文件与要远程加载的文件的组合。

[0358] 在运行第一引导脚本时,大多数的当前数据库结构从来自DB结构存储库38R-06-A的存储库38R-00复制到设备38D-00上的Db38D-04。填充该数据库的数据将经由38P06从DB数据存储库38R-06-B发送到标识信息模块38S-00。可过滤和修改传递通过38S-00的一些数据,以便并入标识信息(诸如Device_ID和其他UUID元素)和以直接复制而无修改的方式传递通过的其他数据。

[0359] 根据设备类型和该设备的通用唯一标识符(UUID),适用于设备 38D-00的数据经由路径38P16而发送到数据库38D-04。一些信息还可能被填入模板配置文件,所述模板配置文件可以被克隆到设备38D-00上的软件和配置文件存储器38D-02。对于设备而言是唯一的标识信息可能包括:设备属性、命名和UUID信息、凭据/密钥、密钥调节器、其他信息。

[0360] 用于系统数据包和其他模块的设置文件将从存储库38R-00上的设置文件存储库38R-02-B克隆并且经由路径38P02发送到设备38D-00上的软件和配置文件存储器38D-02。一些“出厂默认设置”和其他文件还可能经由路径38P10复制到设备38D-0上的安全文件存储器38D06。安全文件存储器38D-06是由GVN的文件和文件夹管理器来管理。需要时来自38D-06的文件还可能经由38P12被克隆至38D-02,诸如在必须返回到出厂设置的情形下。

[0361] 来自存储库39R-00的代码库文件39R-02-A可以经由路径38P00被复制到软件和配置文件存储器38D-02,并且还可以经由路径38P8被复制到安全文件存储器38D-06。

[0362] 上述示出了在首次引导、更新、定期数据交换和其他操作期间的文件和数据从存储库至设备的载入。

[0363] 图39示出了经由两个或更多个EH)将两个LAN桥接为广域网(WAN)。更具体来说,此图示出了经由ETO将两个LAN39-000和39-010 桥接为广域网(WAN)。各个EPD首先经由在其互联网连接之上建立的基站隧道连接至接入点服务器SRV_AP39-200。

[0364] 从EPD39-100,基站连接性路径0TT是经由路径39-P002至存在点 (POP)39-002至互联网39-004至SRV_AP39-200的POP39-006。从 EPD39-110,基站连接性路径0TT是经由路径39-P012至存在点 (POP)39-012至互联网39-014至SRV_AP39-200的POP39-016。

[0365] 从POP39-006至POP39-016的传输路径39-P06可以是通过互联网的路径,藉由经过SRV_AP并且依赖于在公共网络上的路由。若EPD39-100 想要经由互联网连接至39-102,则其可能基于无法控制GVN或EH)的策略沿着不同路由。

[0366] EPD39-100在其自身与SRV_AP39-200之间建立隧道 TUN39-P10oEPD39-102还在自身与SRV_AP39-200之间建立隧道 TUN39-P12。一个或两个这种隧道可能或可能不被加密或被保护。还可以存在另一隧道,内部隧道INTTUN39-P20,所述内部隧道穿过两个其他隧道,在流量可以流过的SRV_AP39-200处接合。此隧道可以是建立WAN 的通信路径。

[0367] 所述隧道和基站连接连接性可以使用不同网络协议。由GVN提供的网络毯式框架可以是不同网络协议的混合,所述网络协议被映射至一系列各种网络节段,同时GVN可以是在内部隧道内的一种网络类型的端对端。

[0368] 图40示出了在GVN上运行的多周界机制(MPFWM)。此实例表明了在全局虚拟网络(GVN)中的元素之上(0TT)可以如何存在第二级40T0P88。在第一级0TT40T0P86处,GVN40-86操作0TT,基站互联网连接性40-82。在多周界防火墙机制40-88构造的情形下,GVN操作0TT并且由此可以被构造为顶部元素之上的第二级40T0P88。

[0369] 图41示出了建立在互联网顶部之上(0TT)的GVN堆栈。此实例描述了建立在互联网41-000之上的GVN41-800堆栈。该图图示了经由隧道 TUN41-100-300和TUN41-100-302的在EPD100与两个SRV_AP服务器 300和302之间的连接性。这样的两个隧道是在EH)与最佳当前接入点服务器(SRV_AP)之间的多个隧道选项的实例,基于服务器可用性和其他因素诸如目的地、流量类型、在起始点与目的地之间的各种网络节段的QoS 和其他。

[0370] 毯式框架41-500将独立网络节段的各种网络协议以及端对端协议编织在一起,所述端对端协议可以是“经过”GVN路径。

[0371] 群集GVN设备41-600表示在GVN设备之间的路由的物理层。

[0372] 经由其他链路41-700的GVN全局网络0TT互联网+是GVN层2逻辑,其中诸如地理目的地、DNS管理、高级智能路由(ASR)/全局 ASR(GASR)、服务器可用性、隧道管理和构建器模块、等等的模块操作。

[0373] GVN41-800表示客户端用户看到的网络。

[0374] 图42将互联网协议IP堆栈B2、0SI模型C2和GVN堆栈C3进行比较。

[0375] IP堆栈由网络接口T1、互联网T2、传输T3和应用T4组成。

[0376] 针对非GVN流量并且针对通过ETHNICN1流出的客户端不可见的物理隧道,由客户端看到的IP堆栈沿着在网络接口T1层处的元素R1、在互联网T2层处的元素R2A、在传输T3层处的元素R3A或R3B和在应用 T4层处的元素R4A、R4B或R4C。

[0377] 针对通过GVN隧道和网络的流量,客户端将在网络接口T1层处的 R4C、在互联网T2层处的R5、在传输T3层处的R6A或R6B、以及在应用T4层处的R7A、R7B或R7C观察到其GVN流

量。

[0378] 尽管OSI模型可能被客户端用于通过隧道的IP流量,GVN具有其自身网络接口G1、互联网G2、传输G3、GVN路由与逻辑G4、GVN互联网G5、GVN传输G6和应用G7的堆栈。

[0379] 逻辑

[0380] 图43示出了国家之间经由众多可能路由的全局互联网流。在全局互联网上的流量在国家之间经由众多可能路由流动,所述路由在对等体之间传输不同互连。

[0381] 在区域诸如亚洲内国家的互联网主要由地面和淹没的海洋链路彼此连接。通常它们在从一个国家至另一国家的流量传输中间的第三或其他国家的地方链接。

[0382] 43-X01表示从亚洲至欧洲的最直接路由。例如经由43-X01从香港至巴黎的延迟时间根据采取的路由将在180ms与250ms之间。

[0383] 43-X02是间接的较长路径,其中通过互联网自然推送流量。此处流量从亚洲经由链路43-P400去往美国西海岸43-400随后经由链路43P402 去往美国东海岸43-402,并且随后经由链路43P600去往欧洲43-600的着陆点。经由43-X02的延迟时间根据欧洲的目的地将为近似396ms至550ms 或更久。

[0384] 在离开区域之前,流量可能在其可以接入国际主干之前必须从一个国家中继至一个或多个其他国家(等)。例如,来自中国43-000的流量可能通过链路43P002运行至中国香港43-002并且随后经由链路43P006运行至日本 43-006。这样的额外区域中跳跃可以将50ms至150ms或更多添加至RTT,甚至在流量离开区域之前。

[0385] 一旦在目的地区域中,流量将在一个国家中例如在UK43-600中从跨大西洋链路43P600着陆。从UK43-600,流量将经由链路43-600运行至法国43-602并随后经由链路43P606运行至德国43-606。这样的额外区域中跳跃可以根据目的地将30ms至更多ms添加到RTT。

[0386] 国际回程质量还可以在对等体之间变化,其中各者具有各种RTTQoS 时间。在正常互联网上的路由和对应速度是决定的中间人参与者,并且这些在基于通常传递慢RTT速度的最低费用的大部分情形下。高延迟时间不是较低质量网络要应付的唯一问题。这些通常具有较高拥塞级别和对应高分组丢失。丢失和缓慢链路显著降低性能。

[0387] 图44再次将互联网协议IP堆栈、OSI模型和GVN网络堆栈进行比较。此实例再次将各种概念性网络模型诸如TCP/IP堆栈B2、开放系统互连模型(OSI)A2C2、还有变化诸如在GVN堆栈A3中的TCP/IP模型、以及 GVNC3的模型进行比较。

[0388] 呈现两种角度。客户端角度A1将A2和A3并列比较。全局虚拟模型架构C1将C2与C3比较。还存在B2的树状连接层。

[0389] 在TCP/IP模型B2中,存在与以太网协议R1对应的网络接口T1。互联网T2与互联网协议(IP)R2对应。传输T3层与TCP协议R3A和UDP 协议R3B对应。其他协议可存在并且在此层操作。此层之上是应用层T4,其中存在超文本传输协议HTTPR4A、邮件服务POP3R4B和GVN应用。其他应用诸如文件传输协议(FTP)或其他服务可以存在于此层中。

[0390] 为了在B2范围中比较TCP/IP模型与OSI模型,OSI数据链路S9和物理链路S8与T1平行。OSI网络S10与T2平行。OSI传输S11与T3平行。

[0391] OSI会话S12、表示S13和应用S14层在R4C,GVN应用的范围内。

[0392] 通过GVNB3的TCP/IP模型建立了至R4C顶部的网络树的延伸。

[0393] 从客户端角度，层T1、T2、T3、T4结合为单个TCP/IP模型层T5，变成用于GVN的中立第三层的网络接口层。这与OSI模型A2物理S1和数据链路S2层进行比较。

[0394] 在R4C之上，存在第三层中的互联网层的表示。互联网IP层于R5 处并且这与互联网T6的A3等级和A2网络等级S3对应。

[0395] TCP协议R6A和UDP协议R6B和此等级与A3等级传输17和A2 等级传输S4对应。其他协议可存在并且在此层操作。

[0396] 从客户端角度T8的应用层与互联网协议诸如FTPR7A、HTTPR7B和 POP3对应。OSI模型将应用层T8拆分为三个层，会话S5、表示S6和应用S7。

[0397] 在GVN的三层模型中，A1描述了在第三层中的操作而B1、B2描述了在第一层中的操作。在T4处的GVN应用R4C和在C1下的操作描述了第二层如何用以允许第三层在第一层之上操作。

[0398] 在GVN的第三层和第一层中的网络操作之间存在相似性。

[0399] 网络连接性NO可以是经由WANN2、专用电路N3、MPLS线路N4 或其他链路至互联网的在定期互联网N1上的其他网络连接性。

[0400] 图45示出了在两个LAN之间经由GVN的隧道。特别地，此图描述了从LAN45-000至LAN45-002通过GVN路径45P00至45P10的内部路径，所述分段通过内部隧道45L300。在两个LAN之间的任一方向中存在对客户端可见的五个跳跃45H0至45H8。通过45L300的路径是对客户端可见的GVN层。

[0401] GVN1级网络层45L100表示针对各种不同类型网络节段端对端的物理网络层。尽管在此图中未表明跳跃数量，并且网络节段至少等于并且最有可能大于在内部隧道45L300中对客户端可见的彼等网络节段。

[0402] 逻辑层2级逻辑45L200是发生各种网络节段整合、路由和其他GVN 操作的逻辑。

[0403] 若客户端路径是通过隧道的IPv6，针对IPv4段而言仅如同45-104，则内部IPv6流量可以此方式封包使得其可以与网络层45L100的网络类型无关地保持固有IPv6端对端。

[0404] 图46将在基站等级经由路径P01至P13的网络与通过GVNT01至 T03的网络进行比较。

[0405] 在基站互联网等级CTN140的大量测量是经由EPD46-100至 SRV_AP46-300的LAN至GVN，针对此测量评估带宽BW、延迟时间 At＝Ams、分组丢失和其他因素的连接性指标。在连接的另一端，在CTN142 的相似测量BW、At＝Cms、分组丢失和其他因素测量了流量从EPD46-102 至GVN中的上升。通过在SRV_AP46-300和SRV_AP46-302之间的GVN，针对GVN跨区域OTT，各种互联网节段CTN340测量了BW、At＝Bms、分组丢失，并且评估其他因素。通过GVN层三GVN4-3的全部路径延迟时间可以被计算为延迟时间的总和A+B+C，全部以毫秒计。

[0406] 在GVN层三GVN4-3，ASR和其他特征支配了流量如何流过GVN 并且在何处流过GVN。这需要确定基于目标区域发送流量的最佳隧道和流量类型、通过GVN的节段的QoS和其他因素。

[0407] 在GVN层一GVN4-1，基站网络连接性的物理条件被监控并测试以确定最佳路由选项，在所述路由选项之上构建GVN隧道和通过其等的路径。GVN路径可以通过相连隧道传输，所述相连隧道经过SRV_AP、SRV_BBX和其他GVN硬件设备。这还可确定继续使用哪些隧道和弃用哪些隧道。

[0408] 在GVN层二GVN4-2的机制、模块和构成部分有助于设置、测试、管理和另外操作在层三GVN4-3与GVN层一GVN4-1之间的管道。隧道测试46-310可以在EPD4100并且在SRV_AP46-300经由其隧道测试器 46-312在层三中完成。

[0409] 图47示出了高级智能路由(ASR)特征以及端点设备(EPD)内的GVN 的地理目的地机制的元素。这包括使用多个DNS源来将流量经由多个路径发送至在世界各个区域中的流出点。在本示例实施例中示出的目标流量区域是:1)本地流量从VIF347-118至互联网47-004保持本地;2)去往其他区域互联网47-002的流量将从VIF147-112通过1'_1102-6至路径47P48 至SRV_AP47-300并随后经由路径47P50至互联网47-002;3)用于其他区域互联网47-006的流量将从VIF247-116通过TUN2102-8至路径47P52至 SRV_AP47-302并随后经由路径47P54至互联网47-006;以及4)用于其他区域互联网47-008的流量将从VIF347-118通过TUN3102-10至路径47P56 至SRV_AP47-304并随后经由路径47P62至互联网47-008。

[0410] SRV_AP47-304包括更多细节以示出其组件AP逻辑47-314和内容拉取代理47-318的一些功能性。此外,EPD100包括更多细节的流程图以示出其内部功能组件。

[0411] 隧道TUN1102-6、TUN2102_8、TUN3102-10和通过VJF具有在虚拟接口VIF147-112、VIF247-116、VIF347-118各者应用的路由表的流量流以与虚拟接口和隧道相似的方式操作。

[0412] DNS高速缓存47-114从多个DNS源经由本地DNS查询机制47-110 通过路径47P38经由47P34播种至互联网47-004至SRV_DNS47-104。远程DNS查询机制47-108可以使DNS请求经由内容拉取代理(CPA)47-318 经由47P44至SRV_DNS47-114。

[0413] 地理目的地机制(Geo-D)经由连接内容传递代理(CDA)47-106与 CPA47-318的47P04将路由信息推送到路由管理器47-104。经由J01的路径47P30至47P40是表示CPA47-318与⑶A47-106一起工作的协调的抽象。在CPA&CDA之间的通信仍是经由隧道和或API调用,或经由链接的高速缓存传输、通过隧道、或可以经由其他机制。

[0414] 在此示例实施例中,通过Geo-D,CPA47-318将全部区域内容从互联网47-008经由47P62拉取至SRV_AP47-304以从寄存目的地内容的主机服务器47-110经由47P66拉取内容,并且在所述内容中CPA47-318可能发现用于其他内容的链路并且CPA47-318将随后从主机服务器47-108经由47P64拉取内容流。其他内容可能经由47P68从主机服务器47_112拉取。通常众多网站将网页寄存在一个服务器上、视频文件从另一服务器流动并且图形从另一服务器提供。

[0415] 图48示出经由GVN采取的多个并行型流量路径的示例。EDGE-1的左侧表示LAN侧。右侧表示互联网面向侧。EDGE-2的右侧表示LAN侧并且左侧表示互联网面向侧。

[0416] 来自LAN001中设备的流量使EPD101经由P002通过加密隧道P003 离开至SRV_AP102并且可以流出至通用互联网106以经由路径H005到达主机客户端或服务器设备D005。来自LAN201中设备的流量使EPD301 经由P103离开至SRV_AP302并且可以经由P106流出至互联网106以经由路径H005到达主机客户端或服务器设备D005。

[0417] EPD101可以经由互联网106通过P003至SRV_AP102至P006至互联网106至P106至SRV_AP302至P103至EPD301链接至EPD301。在 EPD与SRV_AP之间存在经由路径P003和P103的安全隧道。为了确保完全安全性,针对端对端安全隧道,在EPD之间的路径是EPD101至P005 至SRV_AP103至P007至WAN107至P107至SRV_AP302至P105至 EPD301。

[0418] EPD101可以构建经由P003至SRV_AP102的安全隧道并且从彼处经由P201至WAN103至P202至SRV_AP104链接至另一安全隧道，并且随后在远程区域中经由路径P203流出至互联网105并经由路径H002流出至主机客户端或服务器设备D002。

[0419] EPD301可以构建经由P103至SRV_AP302的安全隧道并且从彼处经由P301至WAN303至P302至SRV_AP304链接至另一安全隧道，并且随后在远程区域中经由路径P303流出至互联网305并经由路径H004流出至主机客户端或服务器设备D004。

[0420] EPD101还能够经由在EPD101之间至SRV_102至SRV_AP302至 SRV_AP304的安全隧道到达互联网305中的设备，并且从彼处流出至互联网305。

[0421] EPD301还能够经由在EPD301之间至SRV_302至SRV_AP102至SRV_AP104的安全隧道到达互联网105中的设备，并且从彼处流出至互联网105。

[0422] 存在经由端对端隧道路由、至开放互联网上流出点的隧道、经由多个 SRV_AP设备的隧道和其他选项的众多其他选项。

[0423] 由此示例示出的重要点是由GVN承运的客户端流量是通过GVN第三层，从客户端的角度所述通过GVN第三层与通过互联网的路径相同并且因此能够承运任何类型通过它的流量，尽管仍认识到由GVN提供的改良益处和较高安全度。

[0424] 例如，路径P008示出了在防火墙GW002设备与防火墙GW202设备之间以产生LAN-WAN-LAN网桥的WAN优化连接性。设备与设备间的通信在GVN的第三层内承运并且对GW002和GW202透明。

[0425] 出于简便目的，存在点(POP)网络接入点未在此图中示出。往返于互联网诸如互联网105的至设备D002的路径在H002中间具有POP。

[0426] 在此示例实施例中的WAN表示在互联网之上的GVN设备之间的安全隧道，并且因此任何提及WAN是在GVN的第三层，其中全部GVN流量仍传输第一层。

[0427] 图49描述了从开始处的一个设备49-000到端点设备49-800的自动高级智能路由(ASR)。若路由不可用，则自动高级智能路由可以构建路由，包括但不限于构建新的隧道、以及针对最优化路径来更新内部路由。

[0428] 表1直至表5由此算法用作数据点以出于路由目的使用，诸如确定用于从GVN通过接入点服务器至开放互联网的流量的最佳流出点。此数据还可以由算法用以帮助相对于另一路由区分哪一路由更优先。

[0429] 表1列出从起始点到目的地的各种可用路径并且包括路径排名的评级。

[0430] 表#1-评估通过GVN的各种路由的QoS

[0431]

RT_ID	从起始点到目的地的路径	评分
1	EPD EIP ↔POP↔互联网↔目的地	0.15
2	EPD↔TUN1↔SRV_AP1 EIP ↔POP↔互联网↔目的地	0.36
3	EPD↔TUN2↔SRV_AP2 EIP ↔POP↔互联网↔目的地	0.58
4	EPD↔TUN2↔SRV_AP2↔SRV_AP3 EIP ↔POP↔互联网↔目的地	0.96
5	EPD↔TUN3↔SRV_AP2↔WAN↔SRV_AP4 EIP ↔POP↔ 互联网↔目的地	0.85

[0432] EPD[EIP]和SRV_AP2[EIP]指示从设备到互联网或从互联网到设备的出口/入口点(EIP)。双向箭头符号↔指示在两个设备之间的路由路径。这可以作为互联网之上的网络段,作为隧道或其他机制(可能作为GVN的部分)直接通过互联网或经由设备之间的其他网络路径。起始点在左侧并且目的地意味着流量将路由至或从此路由的最后位置。

[0433] 所述评级是基于数个因素的用于路由的计算值。评级0.00意味着不可能路由。评级1.00意味着在有线线路速度延迟时间具有最高带宽的最佳路由。RT_ID是同时出于实用性、测试和记录目的区分一个路由与另一个的路由ID编号。这用以确定通过GVN的各种路由的质量。RT_ID是来自路由列表的特殊路由的识别符。

[0434] 表2描述了服务器可用性矩阵。

[0435] 表#2-服务器可用性矩阵

[0436]

SA_ID	Server_ ID	IP_Addr _ID	端口	PRI	EPD_ ID	参数	Flag_ State	时间戳
1	8	236	3581	99	1	[阵列]	1	1448674236
2	8	235	19501	98	1	[阵列]	0	1448674237
3	7	218	36152	55	2	[阵列]	0	1448674237
4	5	158	25739	80	1	[阵列]	-1	1448674238
5	19	1672	59081	75	2	[阵列]	1	1448674238

[0437] 在服务器可用性矩阵中保持的信息包括服务器_ID、服务器IP_地址 _ID、端口编号、EPD_ID字段、参数字段(包括安全性和配置设定、状态标志和时间戳)。

[0438] PRI是用以与EPD连接的服务器的加权优先级次序。优先级1是绝对最低优先级。0指示服务器是当前不可到达的。这在Flag_State方面不同,所述Flag_State指示记录是否是当前的。PRI可被保持在相同表中或在另一相关表中,由于PRI是持续变化值并且另一表

将允许历史记录并分析。

[0439] Flag_State为0指示其是备用条目。Flag_State为1指示其是活动的并且其可以被使用。Flag_State为-1指示其已被隐退、不可使用。

[0440] 表3示出了完全路径的延迟时间以及构成网络段的延迟时间。

[0441] 表#3-路由->路径延迟时间评估

[0442]

RT_ID	LAN↔EPD	EPD↔SRV_AP	GVN 传输到出口	出口↔目的地	总的路径延迟	Flag_State	时间戳
1	1 ms	---	---	236 ms	237 ms	1	1448674236
2	1 ms	18 ms	169 ms	12 ms	200 ms	1	1448674237
3	2 ms	23 ms	135 ms	22 ms	182 ms	1	1448674237
4	1 ms	21 ms	139 ms	8 ms	169 ms	1	1448674238
5	1 ms	21 ms	135 ms	19 ms	176 ms	1	1448674238

[0443] 从LAN经由EH)至GVN的路径和或互联网或各种网络节段的组合具有总的路径等待时间,所述等待时间被另外称为RTT,往返时延。所述时间以毫秒计(ms)并用于从起始点到目的地和其返回至起始点的ICMP脉冲。

[0444] 为了评估最佳路由,其可能被拆分为网络节段组,所述网络节段组组成总的网络路径的构成部分。各个节段的评估可以提供关于路由的信息并提供可以使用的数据点。路径评级将总是给予流量额外优先级加权以传输互联网的GVNOTT对传输开放互联网的流量。

[0445] 总的路径延迟时间是以下延迟时间的总和:LAN至EPD加EPD至 SRV_AP加GVN传输加GVN流出至目的地。

[0446] 表4列出路由的服务属性的测得质量。

[0447] 表#4-路由->测量到的QoS因素(当前和历史的)

[0448]

L_ID	RT_ID	Reg_ID	负载	SEC	RTT	R	BW	EFF	其他因素	Flag_State	时间戳
0	1	1	1.5	1.0	1.1	1.00	2.00	1.22	[阵列]	1	1448674236
1	6	1	0.8	1.0	0.9	0.97	0.90	0.80	[阵列]	1	1448674237
2	4	86	1.0	1.0	1.0	1.00	1.00	1.00	[阵列]	1	1448674237
3	5	44	0.7	1.0	0.3	0.50	0.45	0.75	[阵列]	0	1448674238
4	7	49	0.25	0.8	0.8	0.90	0.30	0.95	[阵列]	0	1448674238
5	5	44	0.9	1.0	0.9	0.8	0.78	0.90	[阵列]	1	1448848558
6	9	44	1.0	1.0	1.0	1.0	1.1	1.1	[阵列]	1	1448848559

[0449] 此表被保存为在另一位置和或区域中的源对等体与另一对等体之间的路由的当前和历史QoS(服务质量)结果的日志记录。其可以被实时使用以基于现实状况做出QoS期望决定。此表位于各个起始点设备上并且指示路由性能。

[0450] 各种因素用以评估线路质量比较。此等因素包括系统负载(负载)、安全性(SEC)、往返时延(RTT)、分组丢失(R-可靠性)、带宽(BW)、跳跃计数 (EFF-效率)和其他因素(可用以评估线路参数的值阵列)。

[0451] 采用用于各个点的基线和其间的网络段,以便可以在具有不同硬件配置和网络速度、带宽、以及其他评级的资源之间进行比较。

[0452] L_ID指示用于记录的路由信息的行ID。

[0453] RT_ID是路径id。所述路径可以指示通过基站互联网、通过隧道、接合隧道、或其他GVN相关路由的路径。

[0454] Reg_ID是目标区域ID。

[0455] RTT是基于历史标准的往返时间或延迟时间。值1.0是标准的,而大于1.0指示低于通常延迟时间并且小于1.0指示大于通常延迟时间。

[0456] SEC是安全性评级。值1.0是安全的,且值0.0指示完全不安全和完全折衷的资源。这是基于安全性测试、性能记录和其他数据点。低于1.0 的任何值备受关注。

[0457] R是可靠性并且涉及路由上的分组丢失。例如,R=0.97指示路由上的 3%分组丢失。值R=1.0指示0%数据包丢失和100%可靠性。大于一的评级指示沿着路由发送的分组的平行复制。R=2.0指示针对发送的复制分组的100%可靠性。

[0458] EFF指示就跳跃计数而言相对于路由长度的线路效率并且基于其历史平均值。EFF值1.0意味着标准跳跃计数且小于1意味着大于通常跳跃计数。大于一的值意味着小于通常跳跃计数。

[0459] BW(带宽)基于针对与两点之间的完全网络节段结合的基站连接的线路评级。针对BW的值1.0意味着100％的BW是可用的。值0.5意味着基于路由BW评级仅50％的BW是可用的。并且若值大于一,诸如2.0,则这意味着200％的所述路由的BW容量评级是可用的并且可被采用。例如,针对两点之间的1GigE基站链接,0.55的评级指示550Mbp是可用的。2.0的评级指不可以米用2GigE、等等。

[0460] 在RT_ID＝1的情形下,1.0的SEC(安全性)值指示其是100％安全的,并且大于一的值RTT＝1.1和BW＝2.0指示从一点至另一点的所述路由 RT_ID的连接性具有10％较低延迟时间并且是所述点之间的平均路由的可比较基线性能的带宽的两倍。

[0461] 例如,其中RT_ID＝5,0.80的安全性评级指示存在正在进行的安全性风险,并且0.30的相关可用BW评级显示服务器受到诸如DDoS或强力 (BruteForce)的攻击,其中多个安全性威胁诸如多个并行请求的攻击 (onslaught),所述请求使可用BW(带宽)饱和同时降低SEC(安全性)。

[0462] Flag_State＝1指示当前的活动路由。且Flag_State＝0指示不再使用的历史路由性能。时间戳指示UNIX时间戳的开始时间(自所述时刻的秒数)。

[0463] L_ID＝3*L_ID＝5表明了于两个不同UNIX时间戳1448674238和 1448848558从起始点至区域Reg_ID＝44之间的比较。其显示了随后的性能已经自先前的评级提高。相对于负载＝0.7,负载＝0.9的负载是较佳的,并且基本网络连接性也已改进。

[0464] 此表还可以用以藉由比较各个路由的QoS因素确定从起始点设备至目标区域的两个路由中的较佳路由。例如,L_ID＝5和1_10＝6均指示从起始点至Reg_ID＝44的当前(Flag_State＝l)路由,尽管RT_ID＝5和RT_ID＝9 的路由是不同的。跨此范围的二者中的较佳路由是RT_ID＝9并且应在服务器可用性列表中以较高优先级加权。

[0465] 表5评估并排序在目标区域中的出入点(EIP)。

[0466] 表#5-区域中的EIP

[0467]

EIP_ID	Reg_ID	QoS	BW	负载	S_ID	IP_ID	ATR	Flag_State	时间戳
1	1	0.5	1.0	0.38	25	60	[阵列]	1	1448674258
2	1	6.1	10.0	0.21	39	128	[阵列]	2	1448674258
3	2	0.68	1.0	0.33	50	1851	[阵列]	1	1448674259
4	2	0.14	0.2	0.91	54	1938	[阵列]	-1	1448674270
5	2	0.72	1.0	0.12	68	2188	[阵列]	1	1448674272

[0468] ATR字段是属性字段。这是用以描述EIP规范(RAM、核心、存储空间、其他因素、等等)的属性阵列。S_ID字段保存服务器IDdPJD字段保存IP地址ID。带宽(BW)以GigE测量。例如,20Mbp是0.02,lOOMbp 是0.1且1GigE是1,并且40GigE是40。

[0469] QoS(服务质量)表示用以处理连接和流量的服务器的当前EIP(出入点)适用性。1.0的QoS表示以可接受的可用BW(带宽)和极少直至无负载(服务器的资源负载,RAM、CPU、NIC和其他因素的组合)与EH)连接的服务器的理想状态,

[0470] 小于1.0的QoS意指正被采用的服务器。若QoS接近零,则这意指由于容量饱和其接近全部无用。作为基准并且为了系统健康,小于0.40 的QoS将指示服务器将以更低评级优先排序,以便加权具有更健康QoS 的服务器以在列表上更高呈现并且由此将吸引连接并且不使任何当前服务器过载。

[0471] 此评估和评级机制还可以用作关于如何支持物理基础设施的构建的确定因素。

[0472] 图50示出了低于周界50-832的BB/主干层与高于周界50-822的IP/ 互联网层之间的安全周界50-182。

[0473] 在适当位置存在两重自然保护。第一重保护是将两层接合在一起的唯一方式是经由路径50-TR6B22和50-TR6B32并且必须穿过安全周界。仅有效GVN流量可以在任一方向中经由两个逻辑检查传输。适当位置的其他安全保护是在安全周界50-182之上和之下的网络类型是不同的。

[0474] 图51是全局虚拟网络(GVN)内的高级智能路由(ASR)的流程图。

[0475] 从在连接至端点设备(EPD)103的局域网(LAN)102中的主机客户端 101设备的开始点,GVN提供EPD至多个潜在终端点的大量连接路径。这是流程图是路由逻辑的高级图示,分组可看作其采用ASR传输GVN以用于优化性能。从主机客户端101的角度,其流量将流过互联网协议(IP) 网络,由于GVN的第三层的极少数跳跃和最佳可能延迟时间。GVN的第一层是具有虚拟接口、隧道、路由和其他网络政策的构造的自动配置的基站互联网。GVN的第二层是

[0476] 算法、软件和逻辑支配在层三与层一之间的操作的层。

[0477] 第一主要路由判决是在EP0D内的逻辑门104处,其中流量流出至本地互联网107(此处Ero经由路径P104定位)或若其将经由P107经过安全缠绕并混淆的隧道至接入点服务器(SRV_AP)110,则提供至定位 SRV_AP110的区域的最佳连接性。在流量流出SRV_AP110之前,其经过路由逻辑门111。本地流出至互联网113的流量将经由路径P111去往那里的主机客户端115或主机服务器116。若流量不是本地的而是被中继至另一区域,则其将经由路径P116通过隧道118去往下一SRV_AP119。

[0478] 在SRV_AP119处,众多可能路由选项的三个选项由流量可采取的路径示出。逻辑门126确定流量应保留并且流出至本地互联网129,还是流量应通过隧道经由P126去往另一区域127中的SRV_AP。经由路径P119 示出了另一可能性,其表明从SRV_AP119至远端区域中的另一EPD121 的隧道。这是经由多个桥接隧道桥接的EPD103至EPD121。

[0479] 进一步可能性是流量到达LAN122中的客户端设备125126,其中 EPD121通过EPD的连接P121定位。

[0480] 图52是通过GVN从起始点C 52-002到目的地S52-502可用的各种路由的流程图。可以存在未示出或未论述的更多可能组合。

[0481] 从客户端C52-002至EPD52-108的路径52CP00可以用于测量通过 LAN至ETO的客户端的性能。最佳路由的匹配在测试后并评估可用路径的实时数据来实现。GVN从EPD经由第一跳跃52CP00进入接入点服务器(SRV_AP)52-102、52-104、52-106、52-202、52-204。

[0482] 从EPD至第一SRV_AP的路径可以被定义为从EPD至GVN中的入口点并且由此测量。从SRV_AP至SRV_AP的内部跳跃沿着内部路由,所述内部路由总是尝试维持最佳路径连接性。这些可以是OTT互联网、在主干之上、在暗色光纤之上、或其他相关路由。

[0483] GVN之外的最佳出口点也保持本地追踪,所述本地追踪在该远程区域中并且还整体上用于从起始点至目的地的完整网络段。

[0484] 测试可以考虑到评估的各种因素在各个分段、分段组合和从一端至另一端的总的网络路径上运行。流量类型和路径确定可以根据数据属性和简档QsS需求。主要路径选择总是基于路径之上流量的最佳因素。此机制的功能是匹配在目的地与起始点之间的路径以针对最佳可能双向路由流动。

[0485] 表6是基于IP地址、协议(等)和端口(等)要本地保存的IP地址的列表。

[0486] 表#6-要本地保存的IP地址

[0487]

LRI_ID	IP4_Address	协议	端口	ATR	Flag_State	时间戳
1	36.12.22.88	*	*	[阵列]	1	1448674102
2	204.68.207.18	TCP	80, 443	[阵列]	1	1448674103
3	38.12.251.82	TCP、SCTP、UDP	22	[阵列]	1	1448674258
4	66.220.12.150	UDP	554	[阵列]	0	1448674360
5	8.8.8.8	TCP、UDP	953	[阵列]	1	1448674361

[0488] 此表保存了要本地保存哪些IP地址,使得直接在EPD上或经由与 EPD相同区域中的SRV_AP传输EIP(出口/入口点)。所述

[0489] LRI_ID字段保持本地路由IP地址ID。区域值0指示要本地保存的IP 地址(等)应从EPD从其本地EIP直接去往互联网。区域值1至300指示国家和地区。较高区域ID的区域值表示更细化的粒度。IP4J;也址字段保持IPv4地址。

[0490] 在栏诸如协议或端口下,星号(“*”)意味着通配符涵盖在允许范围中或在允许值列表集合中的全部可能值。如果一个或多个值在一栏中并由逗点分开,那么其指示可以使用一个以上端口、或协议、或其他栏值。则仅明确指出的那些值将受表规定影响,未规定的其他值遵循默认行为。

[0491] 表7是IP地址范围、其目标地理目的地ID和此等规则应用至的 EPDID的列表。

[0492] 表#7-要经由地理目的地路由的IP地址表

[0493]

GDR_ID	IP4_Start	IP4_End	GDReg_ID	EIP_ID	ATR	Flag_State	时间戳
1	8.4.4.2	8.4.4.8	1	1025	[阵列]	1	1448674102
2	201.1.2.5	201.1.2.25	1	1026	[阵列]	1	1448674103
3	38.12.251.82	空	3	3025	[阵列]	1	1448674258
4	66.220.12.76	66.220.12.80	1	1025	[阵列]	1	1448674360
5	151.8.11.1	151.8.15.255	5	5093	[阵列]	1	1448674361

[0494] GDReg_ID字段保持地理目的地ID。区域值0指示要本地保存的IP 地址(等)应从EPD从其本地EIP直接去往互联网。区域值1至300指示国家和地区。较高区域ID的区域值表示更细化的粒度。IP4_Start和IP4_End 字段保持开始和结束IPv4地址。

[0495] 表8是由地理目的地机制采用的国家和其他地理区域的IP地址的基准。由于采用的大量IP地址,采用了CIDR符号。

[0496] 表#8-每区域的IP地址的基准

CIPB_ID	GDReg_ID	区域	CIDR4	Total_IP4	Flag_State	时间戳
1	1	US	3.0.0.0/8	16,777,216	1	1448674102
2	1	US	5.1.94.0/24	256	1	1448674103

[0497]

3	1	US	5.10.70.0/29	8	1	1448674258
4	44	英国	2.22.128.0/20	4096	1	1448674360
5	49	德国	2.16.6.0/23	512	1	1448674361

[0498] 此表根据针对区域路由采用的粒度限定了全国范围块或区域块的IP地址范围。地理目的地路由的地址在区域IP地址表之前按顺序路由并且由此首先路由。

[0499] CIPB_ID字段保持国家IP地址块IDXIDR4栏指示IPv4地址的范围的CIDRXIDR代表无类别域间路由,所述路由是描述IP地址范围的符号。例如,斜线八(/8)符号表示16,780,000个1?地址块。斜线二十(/20)表示 4,096个IP地址。Total_IP4栏指示由CIDR4限定的范

围覆盖的IPv4地址总数。

[0500] 图53是控制从起点设备到端点设备的流量路由选择的算法的流程图。

[0501] 在GVN中,存在用于在GVN设备与各个其他设备诸如EPD和 SRV_AP之间的基本等级互联网的途径的路由表,所述互联网之上可以构建隧道。路由表控制等级1(互联网等级)流量已经于等级3通过GVN的路由。有时,隧道可能不存在或者若隧道存在,其等可能不是最优的。GVN 路由可以根据拓扑数据库被映射至现存和可能的GVN路由。关于基本网络段和设备间的链路的全部信息被存储在GVN数据库中。

[0502] 算法由识别特定GVN流量的目标区域开始。接着,进行检查以查看路径是否通过GVN5306存在。若路径不存在,则构建新的隧道5310。下一步骤是检查隧道5312的健康。若其不健康,则将构建新的替代隧道 5310。一旦健康隧道是可用的,检查路由健康5320。

[0503] 若在目标区域5322中至EIP的路径存在路由并且检查所述路由以查看它对流量类型而目是否是最佳路由。若它是最佳路由,则使用所述路由 5360。

[0504] 若所述路由对数据类型而言是不理想的,则检查以查看是否存在替代 5350。若存在替代,则采用对流量类型而言最佳的路由5352并且使用彼最佳路由5360。当使用路由时,过程评估路由性能5365。在算法完成之前,另一过程将性能数据经由P5328保存在关于服务器可用性、关于 EIP5322的列表还有关于由5302使用的至目标区域的映射路径的日志中。

[0505] 如果于5350的测试确定对数据类型而言路由是不理想的并且不存在替代,将那么经由路径P5314构建新的隧道5310。

[0506] 控制

[0507] 图54示出了GVN中的自动设备协作和信息交换所需的模块。

[0508] EPD100是端点设备。SRV_AP300是位于目标目的地区域中的接入点服务器。SRV_CNTRL200是可由EH)和SRV_AP以及由可能支援图形目的地机制的其他设备访问的中央服务器。

[0509] 各个设备EPD100、SRV_AP200和SRV_CNTRL300将关于自身的信息以列表、文件、数据库表和记录的形式以及其他方式存储在本地信息存储库中。此存储库还包括关于对等体设备关系、储存日志记录的信息以及其他相关操作信息。SRV_CNTRL200还具有额外储存功能并且它的作用是向与其相关的其他设备和/或向可能与其连接的对等体设备提供信息,以便评估当前状态并且提供类似于集中控制的指导,例如发布服务器可用性列表和其他功能。中立API机制(NAPM)可在设备与这些设备的相连对等体之间发送信息,并且还可用以更新API本身。

[0510] 在SRV_CNTRL200上的数据库用作关于自身信息的存储库和用于其他设备的集中存储库。许多位置中可能有许多不同SRV_CNTRL200服务器来充当多主设备。每个数据库可以储存特定信息,包括隧道信息、对等体信息、流量信息、高速缓存信息和其他信息。安全性和其他方面由每个设备独立管理,包括心跳功能、触发脚本和其他机制。

[0511] 图55

[0512] 图55示出了经由GVN的中立API机制(NAPIM)经由路径 API-55A1-55A2、API-55A3-55A2和API-55A1-55A3的EPD100、 SRVCNTRL200和SRVAP300之间的通信。

[0513] 针对将在EPD100与SRV_AP300之间构建的隧道TUN55-1、TUN55_2 和TUN55-3以及针对经由TUN55-5从EPD100至其他SRV_AP服务器诸如TUN55-4和从其他EPD至SRV_AP300的

隧道,在对等体对中的各个设备需要每个隧道的特定信息。

[0514] NAP顶机制存储针对当经由隧道管理器55110和55310构建新的隧道时采用的对等体对的各侧的相关凭据、坐标和其他信息。在 SRV_CNTRL300上的服务器可用性机制55222评估各种隧道的性能,所述隧道经由隧道测试器55112在EH)侧上测试并且通过隧道测试器55312 在SRV_AP侧上测试。来自测试的信息被中继至SRV_CNTRL200上的连接性分析器55288。测试结果包括分配的IP地址和端口组合、使用的端口、来自历史组合使用的结果、来自端口光谱测试的结果和其他相关信息。

[0515] 服务器可用性列表表示具有IP地址列表的EPD100和可由隧道管理器用以构建新的隧道的端口。在列表上提及的SRV_AP300和其他SRV_AP 服务器将被通知期望55320并且收听由EPD100做出的连接尝试。

[0516] 服务器可用性根据构建的隧道的期望最佳性能优先分级SRV_APIP 地址和端口组合的列表,同时还查看可用SRV_AP服务器的当前负载、平衡给予其他EPD的分配列表以及其他可用信息。

[0517] 图56示出了经由NAPIM的GVN设备之间可用的各种类型的通信。

[0518] 闭合环路可用作在已知对等体对之间的NAPIMREQ/RESP通信并且存在两种主要类型;设备至存储库56-P2C和设备至设备56-P2P。

[0519] RESTfulURL公布是对未知对等体(诸如可以分享的通用或一般非敏感信息)的开放访问(若允许彼特定动作)。

[0520] 各个限定的API动作具有控制经由具有可能值的路径类型访问的标志、关于是否需要认证的另一标志、加上其他控制。例如,EPD100可以经由56REQ100200请求可用服务器列表以及对应IP地址和端口并且从 SRV_CNTRL200经由响应路径56RESP100200接收所述列表。同时, SRV_AP300可能经由56REQ100300由EPD100通知或可能经由NAPM、通过数据库复制、经由反向通道、或其他消息从SRV_CNTRL200接收信息。

[0521] 图57描述了全局虚拟网络(GVN)内的不同类型设备之间的API调用组57202、57206和57208。每个API调用实质上是循环式,其中请求从客户端发送到服务器,并且响应发回到客户端。在大多数情况下,客户端可以是对等体对中的一端或另一端,只要另一个对等体已经启用收听功能从而充当服务器即可。

[0522] API调用组57202表示从中央服务器(SRV_CNTRL)200经由路径 P57202-C的调用,到端点设备(EPD)100经由P57202-B的调用以及接入点服务器(SRV_AP)300经由P57202-A的调用。这种类型的通信可以交换在 SRV_CNTRL200和EPD100以及SRV_AP300上的存储库数据库与文件储存器之间交换关于隧道信息、日志信息、计费信息、设备对等体对数据和其他形式的相关信息的信息。

[0523] EPD100与SRV_AP300之间是两种类型的通信路径。它们之间的直接隧道可经由路径P57206-C将第三层流量、信息和二进制文件作为数据包推送。EH)100与SRV_AP300之间还存在经由P57206-B到57206到 P57206-A的路径实现的API调用架构57206。

[0524] EPD100与SRV_AP300之间经由API57206实现的的直接连接可以用于信息共享、协作和验证以及其他信息。例如,重新启动隧道的尝试通常可以由一侧触发,另一侧自动响应并重建它。然而,在隧道被阻塞并且不能重建的情况下,API可以用于发送命令以尝试强制在两端重新启动隧道,并且如果仍然不成功,则可以在设备之间共享信息。该信息可能触发

需要使用新隧道信息来在两个设备之间构建不同隧道,或者使两个设备均向SVR_CNTRL200发送查询以获得新的隧道构建信息。因此,经由API57206 在它们之间建立通信路径是非常有用的。

[0525] API调用组57208表示从CNTRL_SRV200和内部后端基础设施设备以及GVN的其他基础设施支持设备经由路径P57208-C进行的调用。为了简单说明,本示例实施例中示出了一些网关设备,并且此处未示出的GVN 中可能存在经由此路径连接到SRV_CNTRL的其他类型的基础设施设备。

[0526] SRV_GW_电子邮件57310表示电子邮件服务器,并经由P57208-B1 链接到57208,再链接到P57208-C,从而链接到CNTRL_SRV100。可以经由电子邮件网络接入点(NAP)57401发送和接收电子邮件。专用的电子邮件服务器使其他设备能够专注于自己的功能,并且还提供简化的管理,因为它是在电子邮件服务器管理方面唯一需要维护的设备类型。

[0527] SRV_GW_FIN57318表示财务网关服务器,使用该财务网关服务器可经由外部API57501NAP与第三方进行信用卡和其他财务相关交易。与示例SRV_GW_电子邮件一样,专注于单一功能的设备型角色使其他设备能够专注于其核心功能,并提供简化管理,因为只需要对SRV_GW_FIN服务器进行额外的管理以保护与第三方的财务交易。

[0528] SRV_GW_其他57315表示GVN与互联网上的其他服务之间的其他类型的网关。这些类型的网关服务器与SRV_CNTRL200之间的通信经由 P57208-B3到57208到P57208-C实现。

[0529] SRV_AP300与SRV_CNTRL200之间的辅助API路径是经由 P57208-A到57208再到P57208-C,并且出于冗余目的存在并且用于该对等体对之间的基础设施相关通信。

[0530] 来自SRV_AP服务器的另一组调用可经由从P57208-A到57208到 P57208-B1的路径,建立从SRV_AP300到SRV_GW_电子邮件57310的路径;并且经由从P57208-A到57208到P57208-B2的路径,建立从 SRV_AP300到SRV_GW_F1N57218的路径;到并且经由从P57208-A到 57208到P57208-B3的路径,建立从SRV_AP300到SRV_GW_其他57315 的路径。这些可以实现用于直接从SRV_AP300到这些设备进行数据交换的API调用。

[0531] 经由P57208-A传输的API调用也可以表示其他设备经由SRV_AP300 进行的中继API调用,例如经由路径P57206-B到57206到P57206-A到 300到P57208-A到57208到P57208-B2实现的从EPD100到 SRV_GW_FIN57318的调用,在这种情况下,通过SRV_AP300实现的API调用流程只是链中的另一个跳跃,其中客户端是一端EPD100,并且服务器是另一端SRV_GW_FIN57318。

[0532] API调用和其他类型的信息交换对GVN中设备的操作而言至关重要。存在数种类型的自动基础设施操作。这些操作包括:使设备操作系统配置保持最新;从可容纳更新软件的可靠存储库来源更新O/S和模块的软件数据包,以便轻松且可预见地实现修补、更新和最新安装;部署新的全局虚拟网络软件模块并且使已安装的模块保持更新;对GVN数据库进行可控复制;使API操作库保持最新;以及其他操作。

[0533] 在各个设备上,存在后台程序和心搏功能性,其中需要自动化和设备间交互。这包括使后台程序保持运行、使服务保持在线、使队列保持在线以及使其等保持未堵塞、心搏功能、记录功能。

[0534] GVN中的连接性和构造结构包括虚拟接口(VIF)、隧道、多个隧道、路由、服务器可用性、地理目的地、DNS和高速缓存与链接的高速缓存。

[0535] 需要最新的信息来进行隧道建立,并且该信息需要在客户端与服务器之间共享,否则隧道将无法构建。因此,需要进行测试和诊断,同时报告结果数据以进行集中分析,以便了解GVN的整体运作。测试和诊断信息可以包括:第一层条件;隧道的连接性;互联网上的最佳点到点路由;用于最佳路由通过GVN的尚级智能路由(ASR);以及设备操作状态。

[0536] API还可以用于传达关于其自身的信息,例如对等体对信息、队列信息、事务日志、安全/记账和其他日志以及API动作、模式、数据结构以及客户端或服务器上处理动作的相关脚本。

[0537] 也可以经由从设备传输对SRV_CNTRL或其他设备的API调用来传输关于托管服务的状态和配置的信息。此信息可以包括服务在线/离线状态、API模块在线/离线状态并且若可回答,还包括站点的托管状态、数据库状态、安全套接字层(SSL)证书状态、GVN组件状态(例如,诸如地理目的地等组件是否运行)。

[0538] 经由API进行的信息交换存在与安全/FW/监控/协作/信息交换以及 GVN的其他任务关键方面相关的其他用途。API是用于信息交换的强大媒介并且是完整性的自我修复机制,因此可以跨设备部署。

[0539] 图58描述了从客户端设备对等体(源)006发起,通过发送到服务器设备007007B并返回客户端006006B的API调用所采取的步骤。

[0540] API事务在API起始001触发。将数据传递至常见类或其他类型的处理器以创建内部有效负载002。将所述内部有效负载添加到可在存储器中的队列003,将其保存到数据库,平面文件或其他机制中。可以利用立即发送的API调用绕过队列步骤或者可以将该队列步骤设置成在一定时间发送。作为客户端设备006的心搏功能的一部分,并且根据队列中的API 调用的优先级标志,有效负载可以立即处理、在特定时间处理或基于诸如负载、队列003长度、网络条件或其他因素等因素而延迟。当从队列处理项目时,准备好外部有效负载并且针对特殊、单一用途的API调用产生相关事务数据004。当外部APIREQUEST有效负载已准备好被发送时,将所述外部有效负载经由中立API机制005传送,进而通过互联网Q01经由路径CP01至Q01至CP03或通过安全隧道WANQ02经由路径CP02至 Q02至CP04发送到对等体目标007主机(服务器)API。

[0541] 接收008到请求有效负载RP01之后,服务器007将随后开始解析并解释所述有效负载。在处理请求有效负载RP01时,将进行安全性和数据完整性检查并且将解密外部有效负载以发现内部有效负载的内容009。通过对内部和外部有效负载进行比较,将实现进一步安全性和数据完整性检查。验证之后,将有效负载传送到对应的脚本以采取规定的动作010。在完成请求动作时,创建用于响应的内部有效负载011。外部有效负载创建 012和事务准备013采用创建API请求外部有效负载RP01时所采用的相同过程来创建外部APIRESPONSE有效负载RP02。随后经由中立API014 发送回响应。

[0542] APIRESP(响应)RP02沿着相同路径从API服务器007返回API客户端006。

[0543] 由对等体源API客户端设备006接收回015APIRESPRP02。解析016 并处理017有效负载。根据API动作类型,接收回的数据将被传送到006 上的API处理器脚本。记录全部事务018。

[0544] 如果规定020回调019,那么将经由路径P019发起并且经由路径P020 并行新的调用,原始API调用在API完成022处完成。

[0545] 如果在APIRESPRP02中未规定021回调,则原始调用经由P021进行至终止点022以完成该事务。

[0546] 图59是示出EPD与SRV_AP之间用于获得地理目的地功能性的交互的流程图。具体来说,此图描述了地理目的地机制的处理流,该流程开始于客户端000并且沿着顺次序且有时并行的通信路径从CP0到达步骤12 端点设备(EPD100),其中EPD100与接入点服务器交互(SRV_AP300)。

[0547] 当已将远程区域内的内容拉取至SRV_AP300并随后经由传输及在地理目的地机制内的高速缓存发送回EPD100,进而在步骤15中经由路径 CP203提供回客户端000时,此处理流结束。

[0548] 步骤8中,经由CP13、CP14、CP12从内容服务器SRV803、804、802并行地拉取内容,并且将结果经由CP10发送回以用于列表并随后处理数据拉取。

[0549] 步骤1、12、13和15相对于客户端000和EPD100在原始区域中发生。

[0550] 步骤2、10、11和14是在EPD100与SRV_AP300之间的任一个或两个方向中传输时发生的步骤。

[0551] 步骤5、6和9在SRV_AP300上发生。

[0552] 步骤3、4、7和8从SRV_AP300、在该SRV_AP300所在的远程区域中的互联网上经由EIP(出口/入口点)发生。

[0553] 步骤3用于对客户端000请求的内容的初始URL、URI和URN进行 DNS查找。步骤7用于DNS查找作为初始拉取内容的构成部分而拉取的嵌套内容。

[0554] 图60描述了地理目的地内的设备协作,总体来说组成部分指示为模块并且在各个设备上提及的其构成部分包括存储在记忆体和数据库中的信息和信息交换,以及针对API流量以及数据传输诸如设备间的文件传输经由通信路径通信的信息。GVN使得能够控制跨多个设备延伸的复杂自动结构一起工作以实现共同目标。

[0555] 该图示出了EPD100的组件并且示出了在端点设备(EPD)上的地理目的地机制。该图还示出了SRV_AP300的组件并且示出了在来自EPD的远程区域中的接入点服务器(SRV_AP300)上的地理目的地机制。

[0556] 内容拉取代理D302位于SRV_AP300上。CPAD302从位于EPD上的 CDAD102接收目标URL/URI。客户端希望到达的此目标地址位于来自客户端的另一区域中并且是客户端希望拉取内容的位置。CPAD302将请求地址传送至远程抓取器BOT(R.F.BOT301)。

[0557] R.F.BOTD301的工作是进行DNS查找D304并且随后使用所述信息经由数据拉取301来拉取内容。R.F.BOTD301经由CP01与CPAD302协作以解析抓取结果,进而查找辅助内容的任何其他地址,所述辅助内容可以并且应作为该内容的构成部分拉取。将请求存储在数据库D302中以供 CPAD302和R.F.BOTD301访问并进一步参考。将内容文件列表L301从R.F.BOTD301传送到CPAD302。将数据文件内容从数据拉取301经由 R.F.BOTD301传送到高速缓存管理器D303。将拉取的文件发送到高速缓存管理器D303以用于作为文件聚集或作为独立文件传输。

[0558] 根据从起始点到地理目的地区域的距离、文件类型和QoS,在高速缓存中拉取的文件可能聚集为通过链式高速缓存统一传输的单个文件或者可以以作为并行并发流形式发送的独立文件。

[0559] 存在多个到远程区域的可选路径。数据可以经由在API与TP01至 TP02之间的路径、在TP01与TP03之间的路径、以及在TP02与TP03之间的路径传输。数据文件还可以通过GVN经由路径CP38、CP39或P06 至CPBB等等传输。CP38是从SRV_AP300经由GVND888至SRV_APD555 的经由隧道的路径。CPBB是在SRV_APD555与SRV_AP300之间经由中继SRV_APD505路径P06的主干路径。CP39是在GVN之上从高速缓存 701经由SRV_APD555至EPD100的文件传输路径。CP02指示SRV_AP300 与EPD100之间的直接连接路径可能性。

[0560] 基于当前状况、网络分段属性和这些属性如何贡献于最佳传输、数据类型以及其他因素，到达远程区域的可选路径提供了流量经由最佳路由流动的选项。

[0561] 图61示出了全局分布的平行文件系统(PFS)如何经由GVN连接。具体来说，此图示出了全局分布的平行文件系统(PFS)可如何允许使用本地 RDMA接入通过在各种非本地网络光纤顶部之上(OTT)的GVN越式框架 (Tapestry)无缝地接入三个61308、或61318或61328PFS存储节点中的一个节点，以实现所需服务质量(QoS)并且符合此功能性所需的高性能计算 (HPC)原理。

[0562] PFS61308是链接至“云端中”的两个其他PFS实例的EPD之后的客户端LAN中一个PFS实例的示例，其中全部三个PFS存储节点之间的IB 之上的本地RDMA允许真正地并行接入，不论基本分段处的网络类型是什么。链路61CP06是EPD100和SRV_AP300之间的基本互联网连接并且TUN1在61CP06的OTT运行。61CP10在IDC或OTT互联网之内。PFS61308经由路径61CP08->8CP02->8CP06/TUN1->8CP10->8CP12_>8CP18连接至 PFS61318，所述路径表示区域内的短距离。这些设备均位于相同高性能区内。

[0563] SRV_AP300经由61CP10连接至SRV_BBX61310并且二者均位于相同全局节点内。

[0564] PFS61318经由连接至SRV_BBX61320的SRV_BBX61310连接至 PFS61328，这表示经由GVN的全局节点至全局节点的远距离通信。

[0565] 本发明的范围不限于本文描述的特定实施例。事实上，除了本文中描述的内容之外，本领域中的普通技术人员可以从以上描述内容和附图清楚地了解到本发明的其他多个实施例和对本发明的修改。因此，此类其他实施例和修改预期在本发明的范围内。此外，尽管本发明已经在针对至少一个特定目的的至少一个特定环境中的至少一个特定实施例的上下文中进行了描述，但是本领域中的普通技术人员将认识到本发明的有用性不限于此，并且本发明可以在出于任何数量的目的在任何数量的环境中有益地实现。因此，所附权利要求书应根据本文所述的本发明的完整广度和精神来解释。

[0566] 根据本公开的实施例，还公开了以下附记：

[0567] 1.一种用于经由全局虚拟网络来连接设备的网络系统，包括：

[0568] 与第一端点设备通信连接的第一设备；

[0569] 与第二端点设备通信连接的第二设备；以及

[0570] 连接所述第一端点设备和第二端点设备的通信路径，所述通信路径还包括一个或多个中间隧道，所述一个或多个中间隧道将每个端点设备连接到一个或多个中间接入点服务器以及一个或多个控制服务器。

[0571] 2.根据附记1所述的网络系统，其中所述第一端点设备和所述中间接入点服务器中的至少一个被配置用于执行域名系统查找以便定位所述第二设备。

[0572] 3.根据附记1所述的网络系统，其中所述第一端点设备和所述中间接入点服务器

中的至少一个被配置用于从高速缓存中执行域名系统查找以便定位所述第二设备。

[0573] 4.根据附记1所述的网络系统，其中所述中间接入点服务器中的至少一个被配置用于缓存内容。

[0574] 5.根据附记1所述的网络系统，其中所述端点设备和所述中间接入点服务器中的至少一个被配置用于执行智能路由。

[0575] 6.根据附记5所述的网络系统，其中所述智能路由基于最佳带宽、最低延迟时间、最少跳跃和无分组丢失中的至少一个。

[0576] 7.根据附记5所述的网络系统，其中所述智能路由基于实时统计和历史统计中的至少一个。

[0577] 8.根据附记1所述的网络系统，其中所述端点设备和所述中间接入点服务器中的至少一个被配置用于执行防火墙服务。

[0578] 9.根据附记8所述的网络系统，其中所述第一端点设备在所述第一设备与所述中间接入点服务器之间提供防火墙服务。

[0579] 10.根据附记8所述的网络系统，其中中间接入点服务器在第一端点设备与其他中间接入点服务器或所述第二端点设备之间提供防火墙服务。

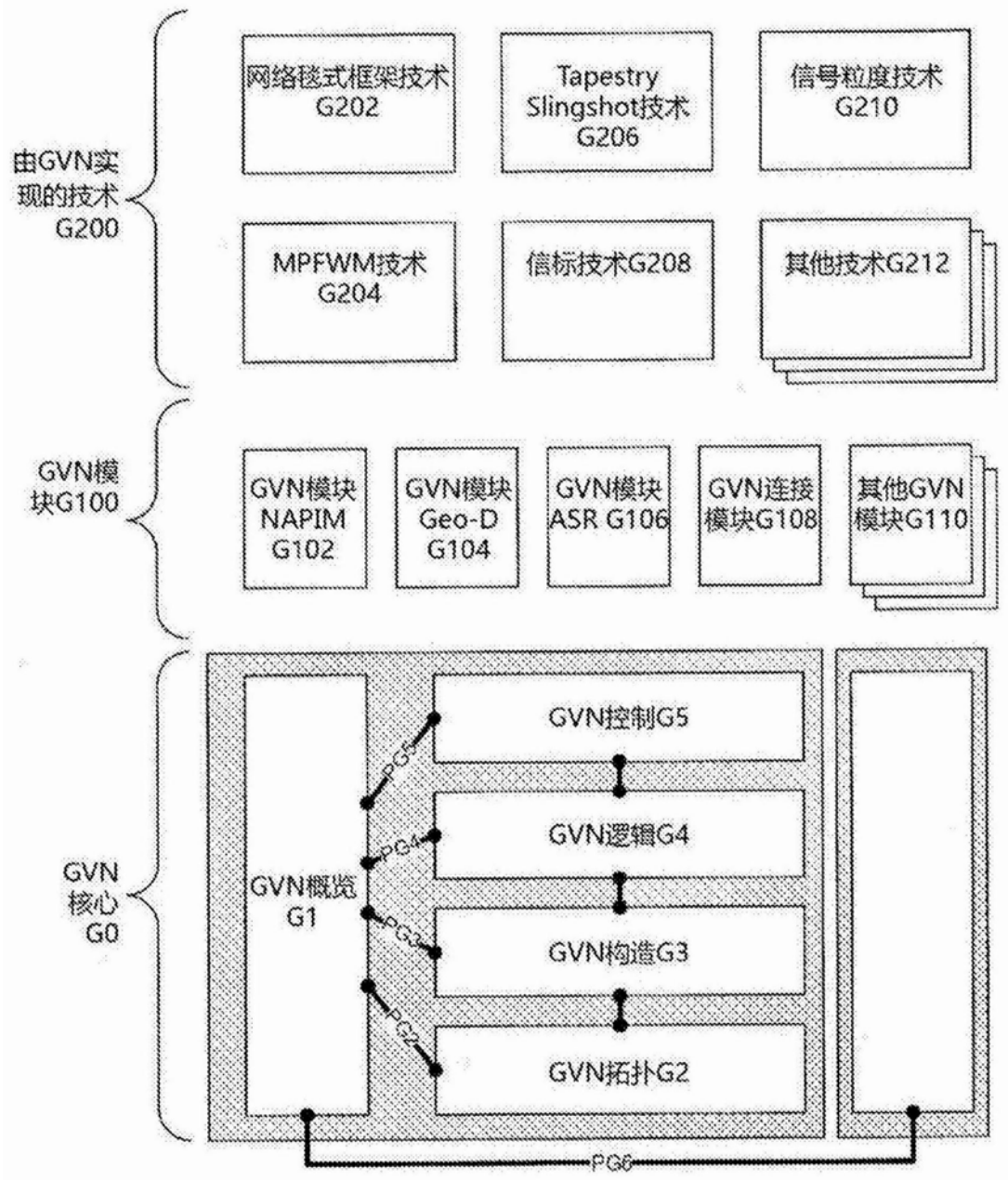

由GVN实现的技术G200
网络毯式框架技术G202
Tapestry Slingshot技术G206
信号粒度技术G210
MPFWM技术G204
信标技术G208
其他技术G212
GVN模块G100
GVN模块NAPIM G102
GVN模块Geo-D G104
GVN模块ASR G106
GVN连接模块G108
其他GVN模块G110
GVN核心G0
GVN概览G1
GVN控制G5
GVN逻辑G4
GVN构造G3
GVN拓扑G2
PG5
PG4
PG3
PG2
PG6

图1

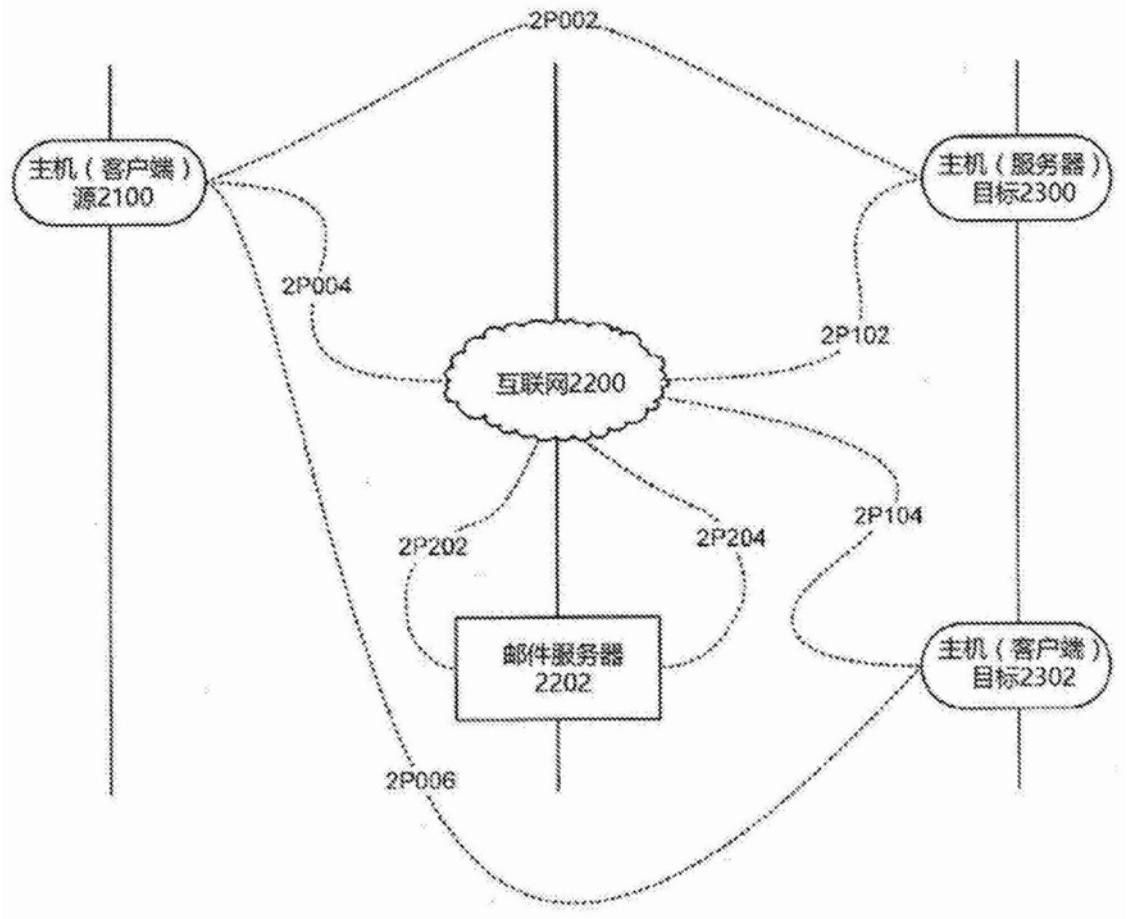

2P002
主机（客户端）
源2100
主机（服务器）
目标2300
2P004
2P102
互联网2200
2P104
2P202
2P204
邮件服务器
2202
主机（客户端）
目标2302
2P006

图2

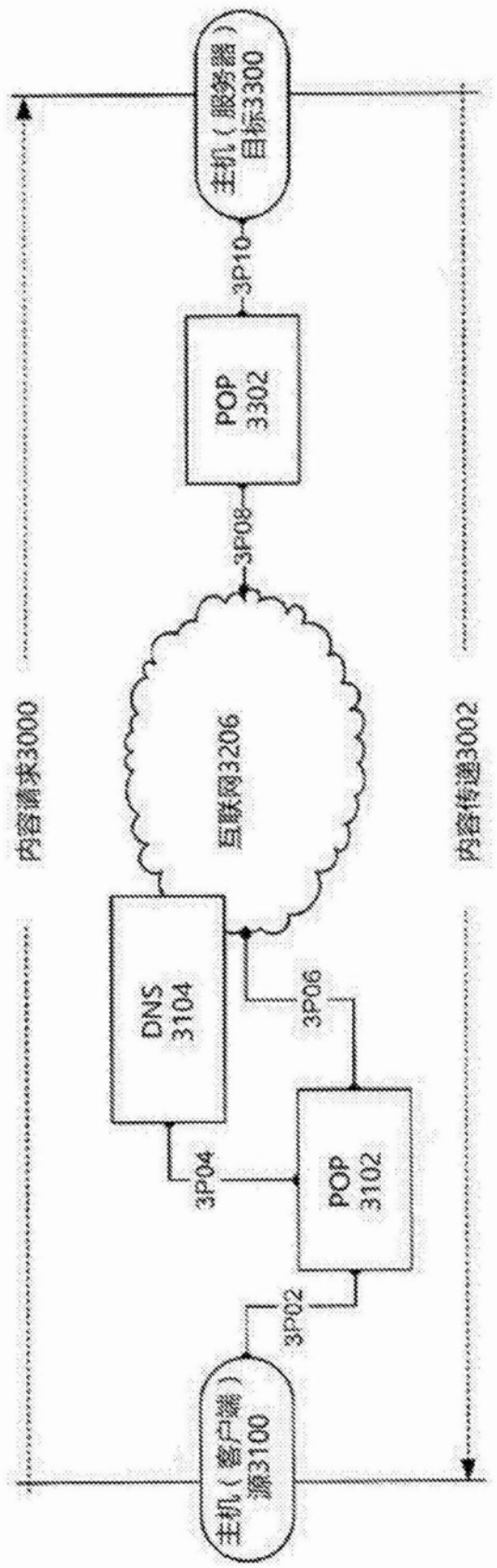

主机（服务器）
目标3300
3P10
POP
3302
3P08
互联网3206
内容请求3000
内容传递3002
DNS
3104
3P06
3P04
POP
3102
3P02
主机（客户端）
源3100

图3

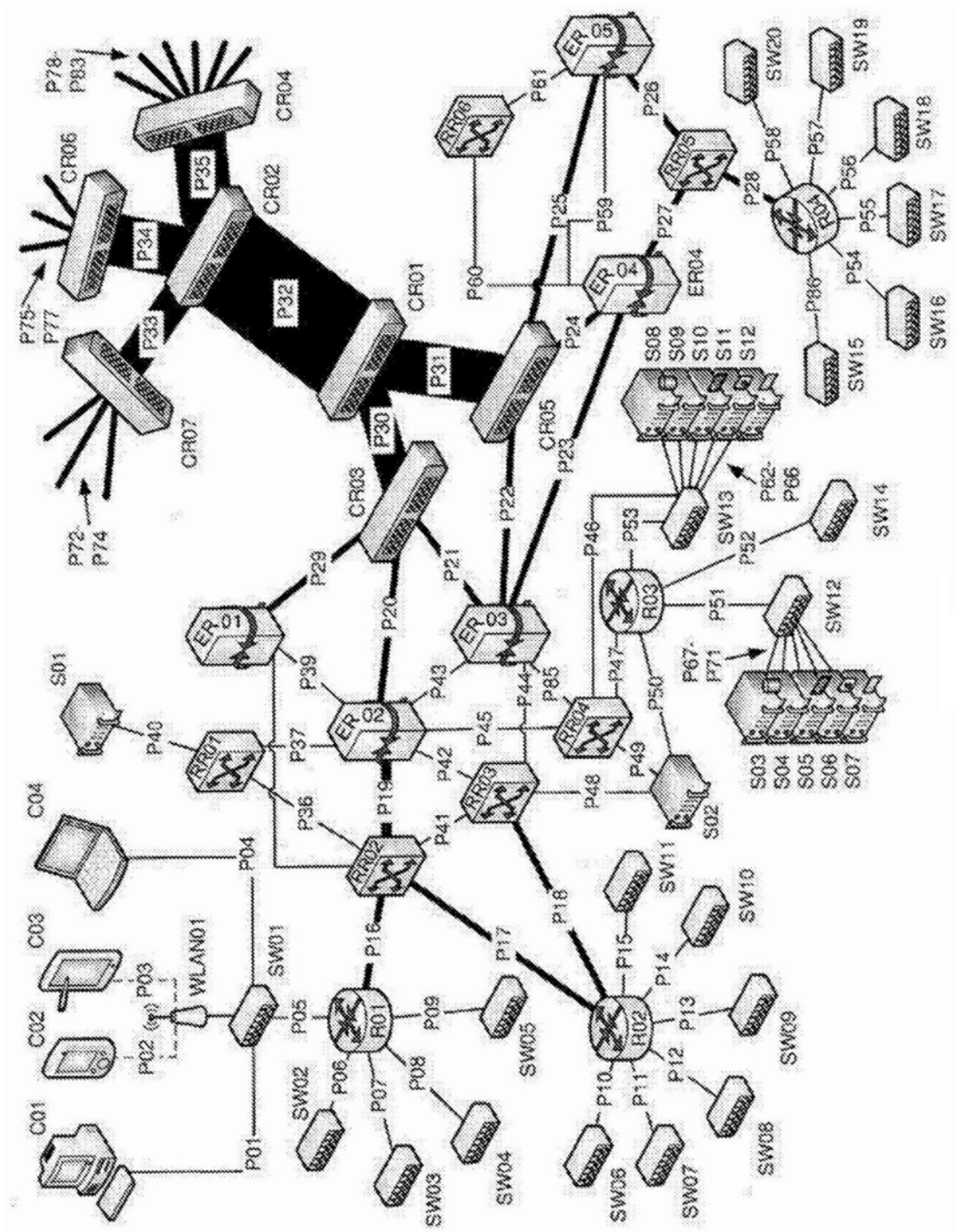

CR01
CR02
CR03
CR04
CR05
CR06
CR07
ER01
ER02
ER03
ER04
ER05
RR01
RR02
RR03
RR04
RR05
RR06
RR07
R01
R02
R03
R04
WLAN01
SW01
SW02
SW03
SW04
SW05
SW06
SW07
SW08
SW09
SW10
SW11
SW12
SW13
SW14
SW15
SW16
SW17
SW18
SW19
SW20
C01
C02
C03
C04
S01
S02
S03
S04
S05
S06
S07
S08
S09
S10
S11
S12
P01
P02
P03
P04
P05
P06
P07
P08
P09
P10
P11
P12
P13
P14
P15
P16
P17
P18
P19
P20
P21
P22
P23
P24
P25
P26
P27
P28
P29
P30
P31
P32
P33
P34
P35
P36
P37
P39
P40
P41
P42
P43
P44
P45
P46
P47
P48
P49
P50
P51
P52
P53
P54
P55
P56
P57
P58
P59
P60
P61
P62-P66
P67-P71
P72-P74
P75-P77
P78-P83
P85

图4

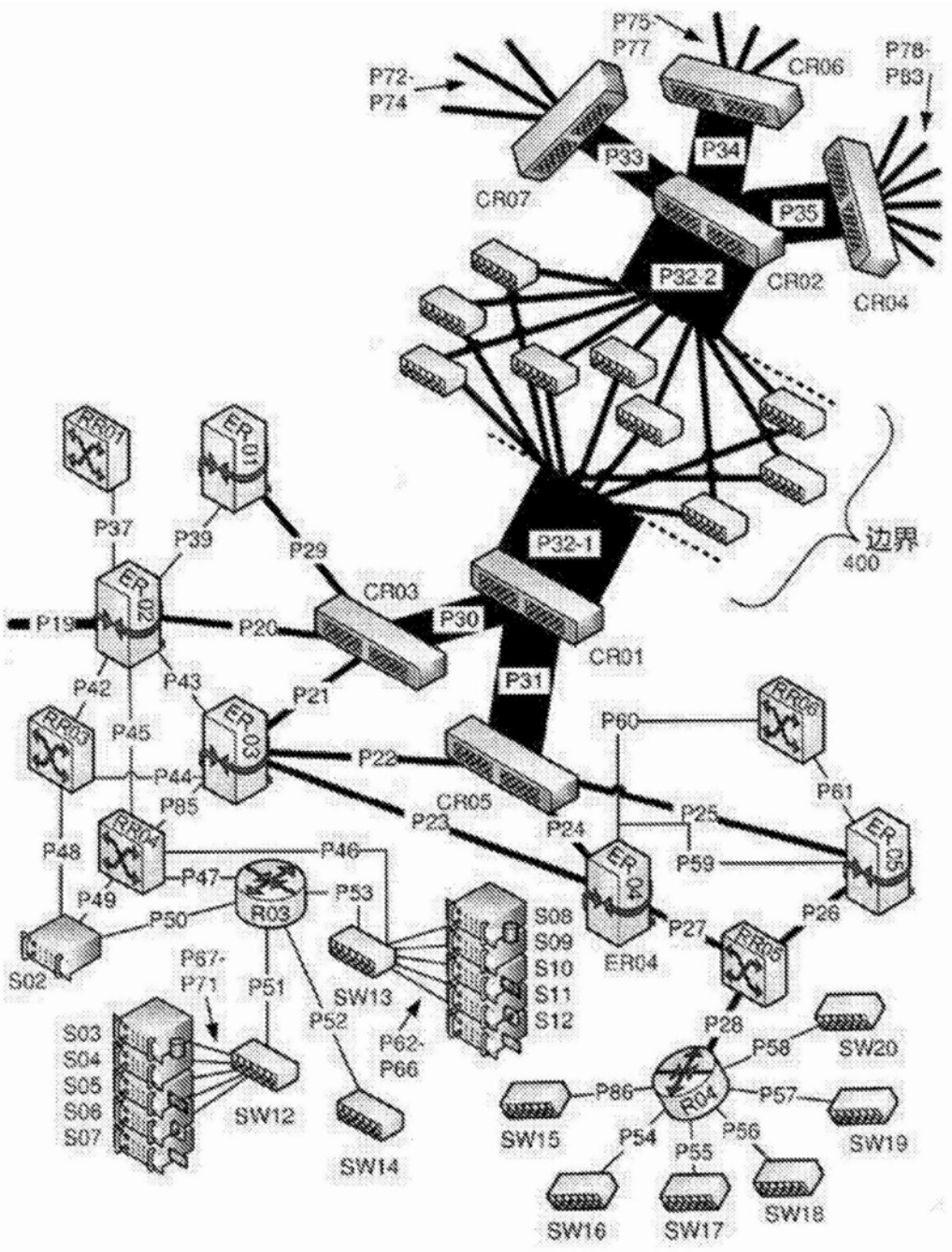

P75
P77
CR06
P78-
P83
P72-
P74
P33
P34
CR07
P35
P32-2
CR02
CR04
RR01
ER01
P37
P39
P29
P32-1
边界
400
ER02
CR03
P19
P20
P30
CR01
P42
P43
P21
P31
RR02
P45
ER03
P60
RR05
P22
P44
P61
P85
CR05
P23
P24
P25
RR04
P48
P46
ER05
P59
P47
P49
R03
P53
P26
P50
S08
S09
S10
S11
S12
ER04
P27
S02
P67-
P71
P51
SW13
RR06
P52
P62-
P66
P28
S03
S04
S05
S06
S07
SW12
P58
SW20
P86
R04
P57
SW15
P54
P55
P56
SW19
SW14
SW16
SW17
SW18

图5

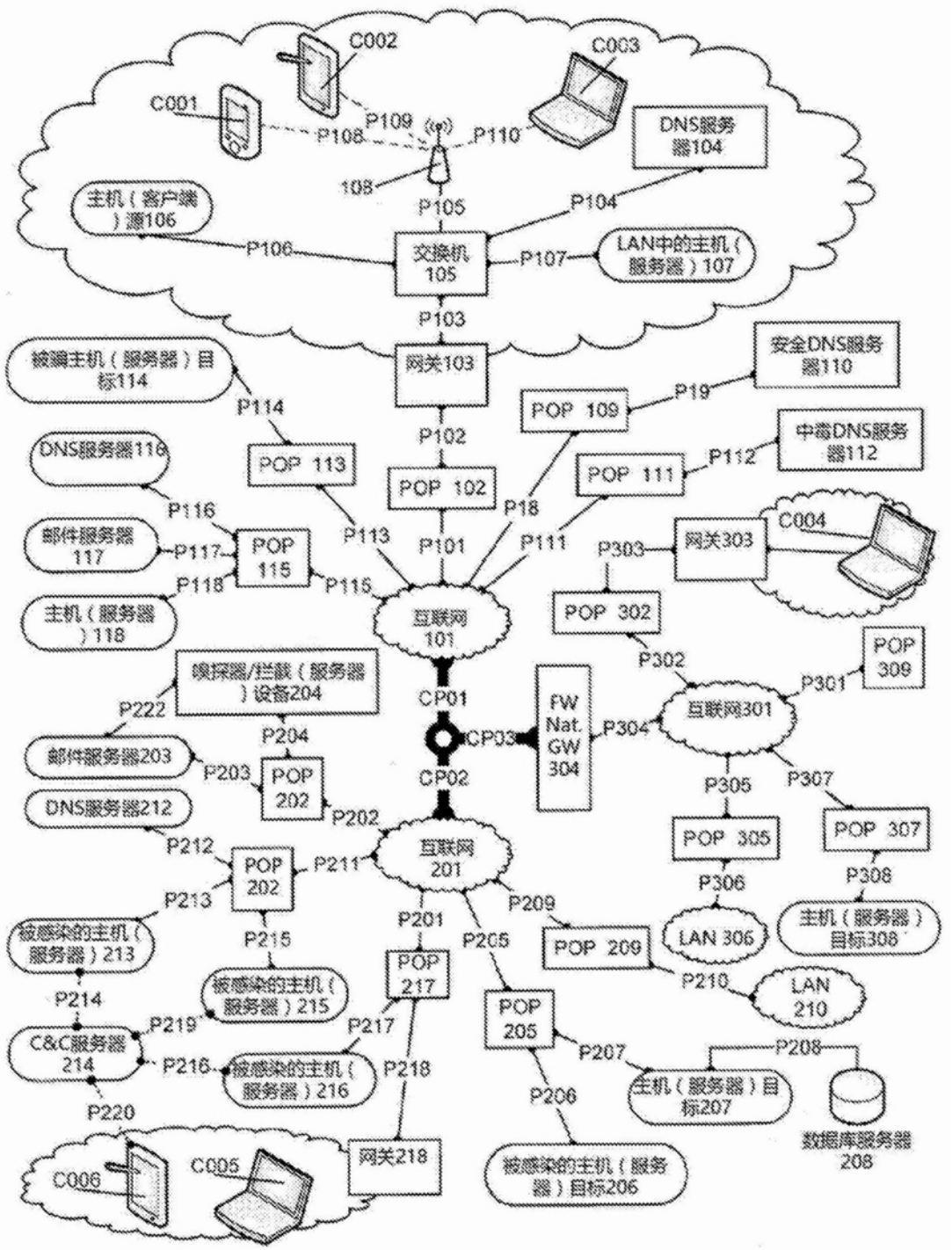

C002
C003
C001
P109
P108
P110
DNS服务器104
108
P105
P104
主机（客户端）源106
P106
交换机105
P107
LAN中的主机（服务器）107
P103
网关103
被骗主机（服务器）目标114
安全DNS服务器110
P19
P114
POP 109
P102
DNS服务器118
POP 113
POP 102
POP 111
P112
中毒DNS服务器112
P116
P18
邮件服务器117
P117
POP 115
P113
P101
P111
P303
网关303
C004
P118
P115
主机（服务器）118
互联网101
POP 302
POP 309
P302
P301
嗅探器/拦截（服务器）设备204
CP01
FW Nat. GW 304
P222
互联网301
P204
CP03
P304
邮件服务器203
P203
POP 202
CP02
P305
P307
DNS服务器212
P202
POP 305
POP 307
P212
互联网201
P306
P308
POP 202
P211
P213
P209
主机（服务器）目标308
被感染的主机（服务器）213
P201
P205
POP 209
LAN 306
P215
POP 217
P210
LAN 210
被感染的主机（服务器）215
P214
POP 205
P219
P217
P207
P208
C&C服务器214
P216
被感染的主机（服务器）216
P218
主机（服务器）目标207
P206
P220
数据库服务器208
C006
C005
网关218
被感染的主机（服务器）目标206

图6

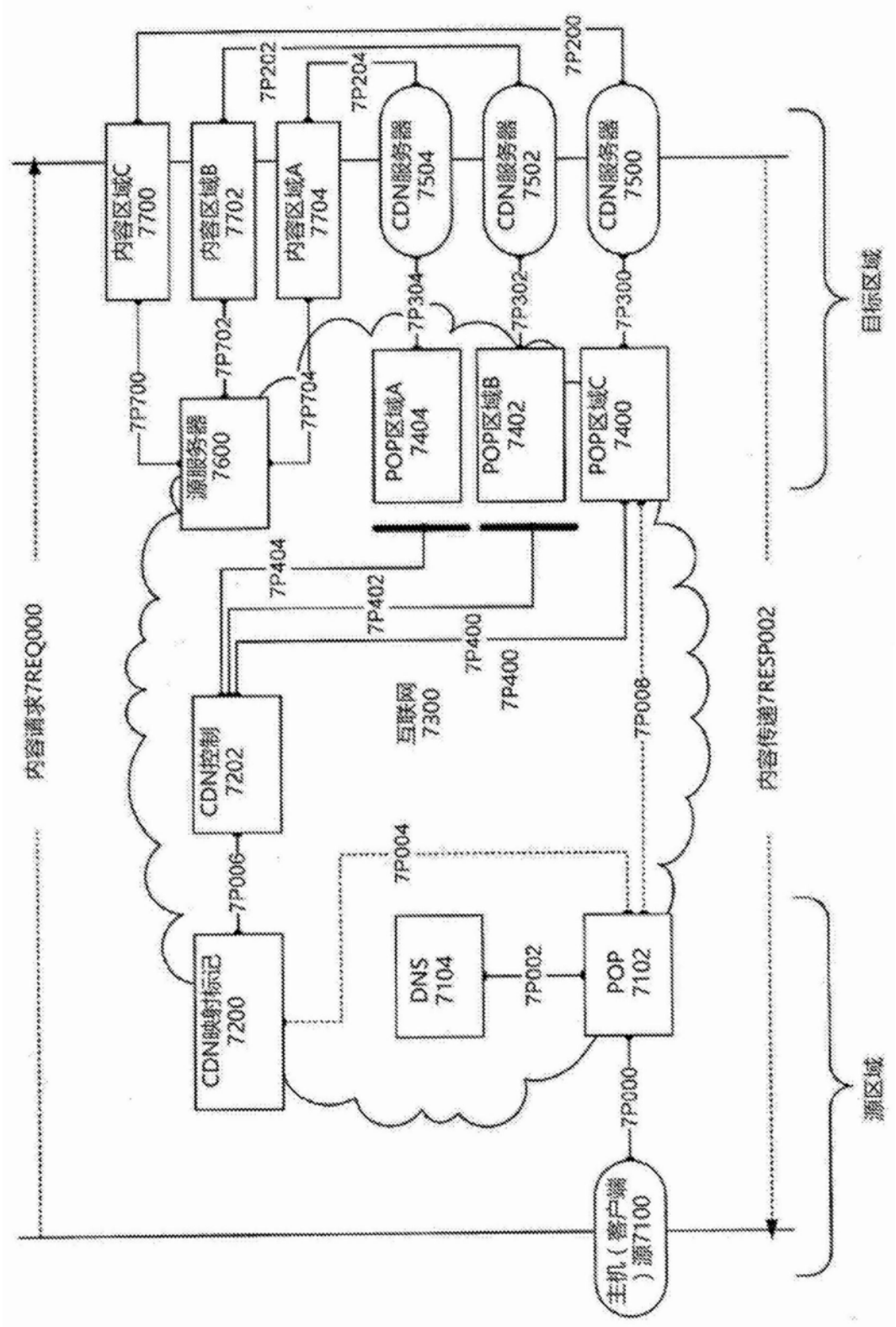

内容区域C 7700
内容区域B 7702
内容区域A 7704
CDN服务器 7504
CDN服务器 7502
CDN服务器 7500
7P202
7P204
7P200
7P304
7P302
7P300
7P702
7P704
7P700
源服务器 7600
POP区域A 7404
POP区域B 7402
POP区域C 7400
目标区域
7P404
7P402
7P400
7P400
互联网 7300
CDN控制 7202
7P008
内容请求7REQ000
内容传递7RESP002
7P006
7P004
CDN映射标记 7200
DNS 7104
7P002
POP 7102
7P000
主机（客户端）源7100
源区域

图7

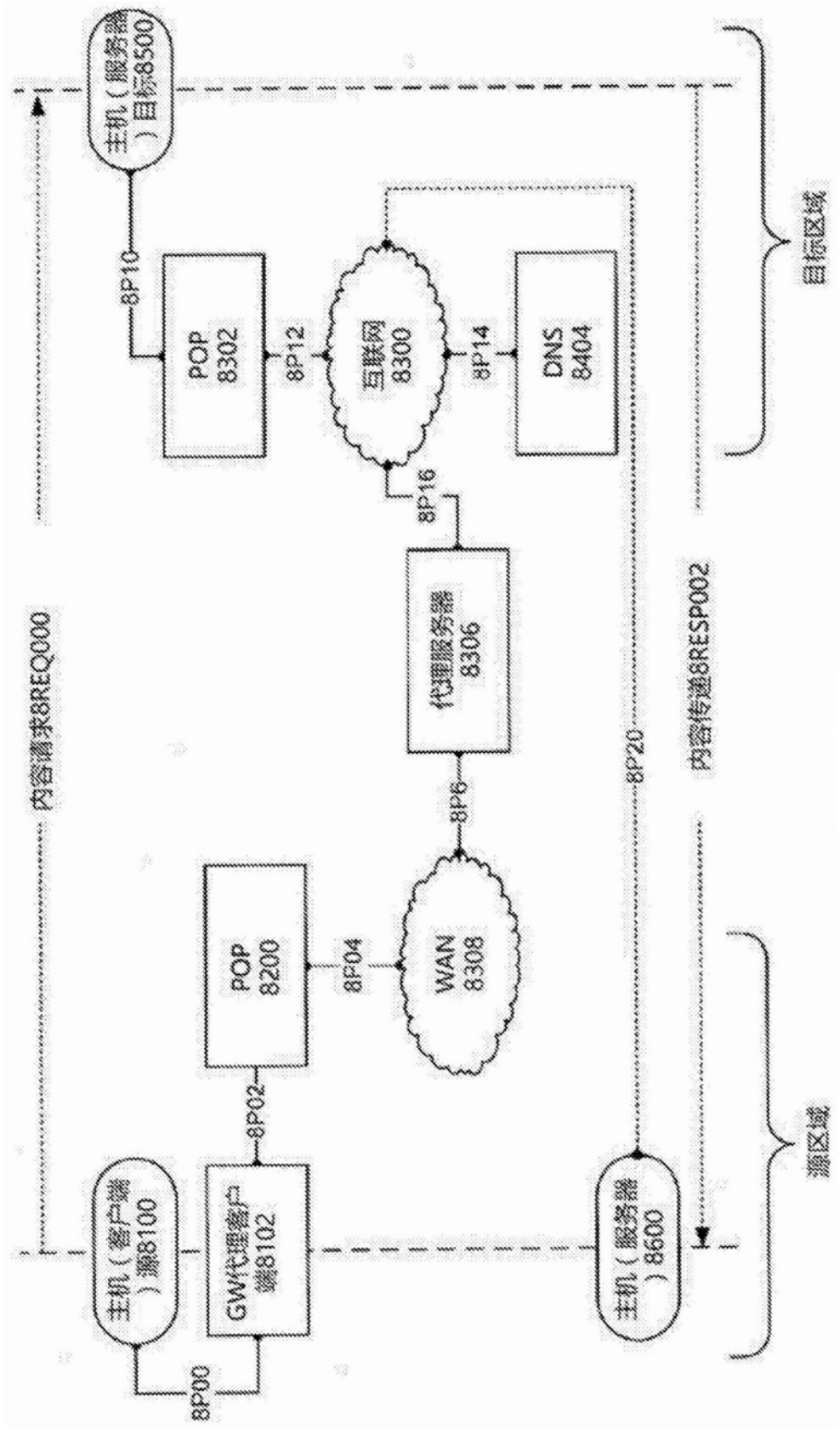

主机（服务器）目标8500
8P10
POP 8302
8P12
互联网 8300
8P14
DNS 8404
目标区域
8P16
代理服务器 8306
8P6
内容请求8REQ000
内容传递8RESP002
8P20
POP 8200
8P04
WAN 8308
8P02
主机（客户端）源8100
GW代理客户端8102
主机（服务器）8600
源区域
8P00

图8

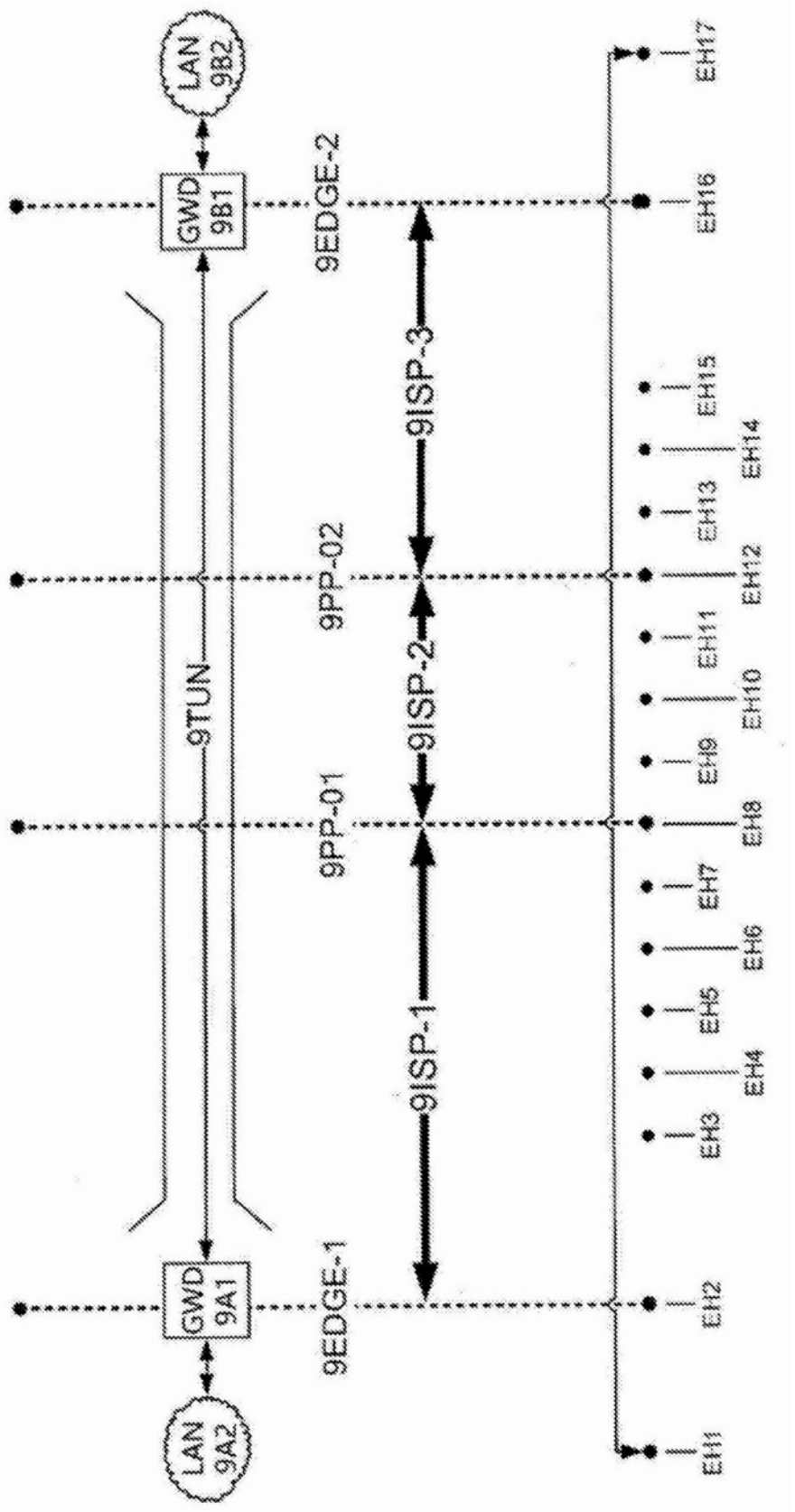

LAN
9B2
GWD
9B1
9EDGE-2
9PP-02
9PP-01
9EDGE-1
GWD
9A1
LAN
9A2
9TUN
9ISP-3
9ISP-2
9ISP-1
EH17
EH16
EH15
EH14
EH13
EH12
EH11
EH10
EH9
EH8
EH7
EH6
EH5
EH4
EH3
EH2
EH1

图9

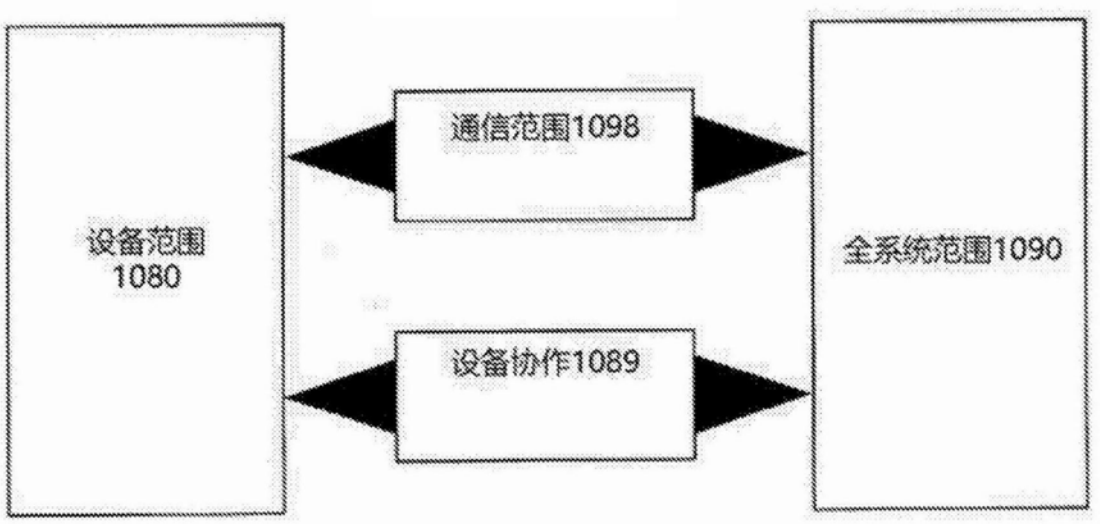


图10

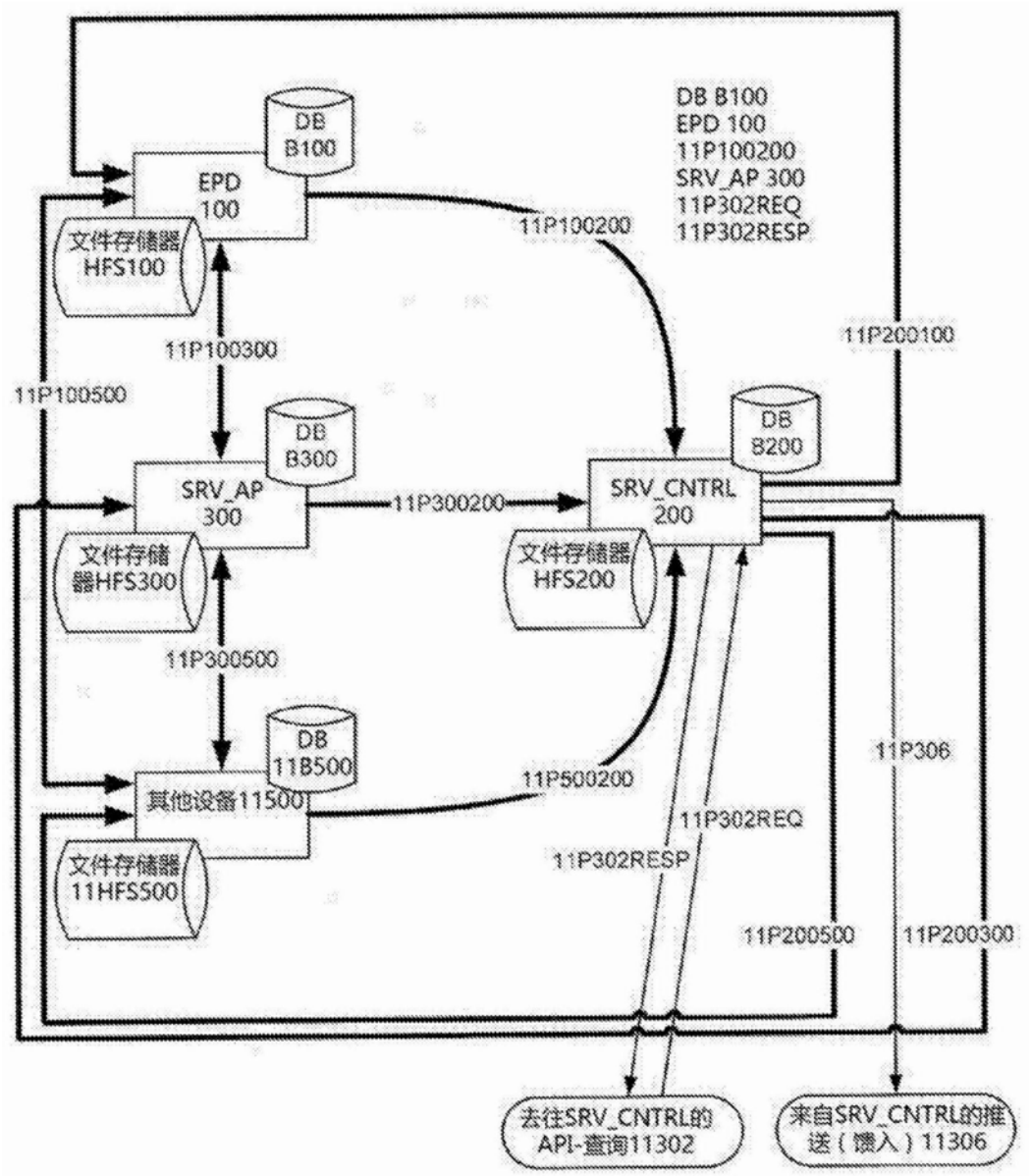

DB B100
EPD 100
11P100200
SRV_AP 300
11P302REQ
11P302RESP
DB B100
EPD 100
文件存储器 HFS100
11P100200
11P200100
11P100300
11P100500
DB B300
SRV_AP 300
11P300200
DB B200
SRV_CNTRL 200
文件存储器 HFS200
文件存储器HFS300
11P300500
DB 11B500
其他设备11500
11P500200
11P306
11P302REQ
11P302RESP
文件存储器 11HFS500
11P200500
11P200300
去往SRV_CNTRL的API-查询11302
来自SRV_CNTRL的推送（馈入）11306

图11

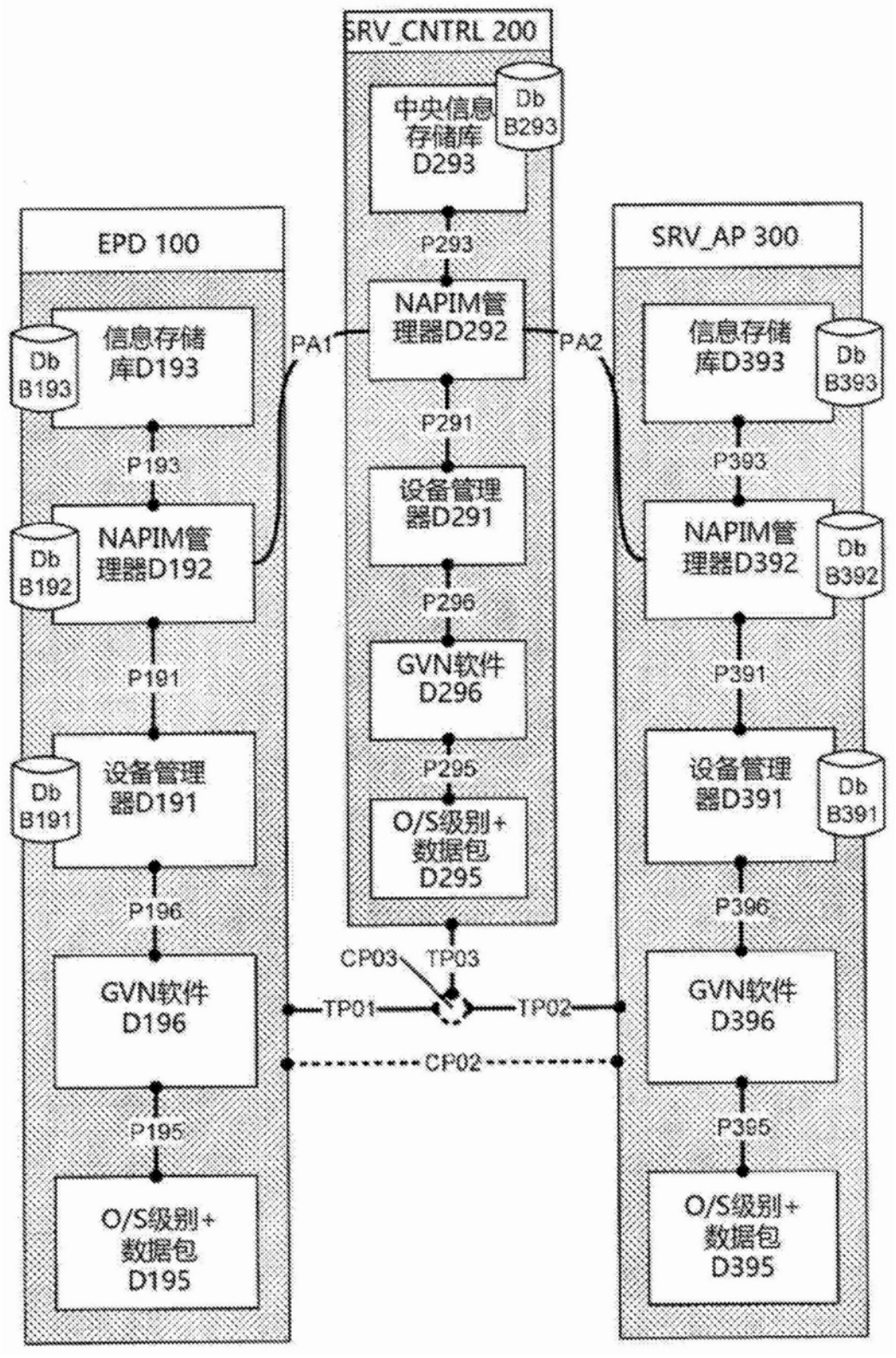

SRV_CNTRL 200
中央信息存储库D293
Db B293
P293
NAPIM管理器D292
P291
设备管理器D291
P296
GVN软件D296
P295
O/S级别+数据包D295
CP03
TP03
TP01
TP02
CP02
EPD 100
信息存储库D193
Db B193
P193
NAPIM管理器D192
Db B192
P191
设备管理器D191
Db B191
P196
GVN软件D196
P195
O/S级别+数据包D195
PA1
SRV_AP 300
信息存储库D393
Db B393
P393
NAPIM管理器D392
Db B392
P391
设备管理器D391
Db B391
P396
GVN软件D396
P395
O/S级别+数据包D395
PA2

图12

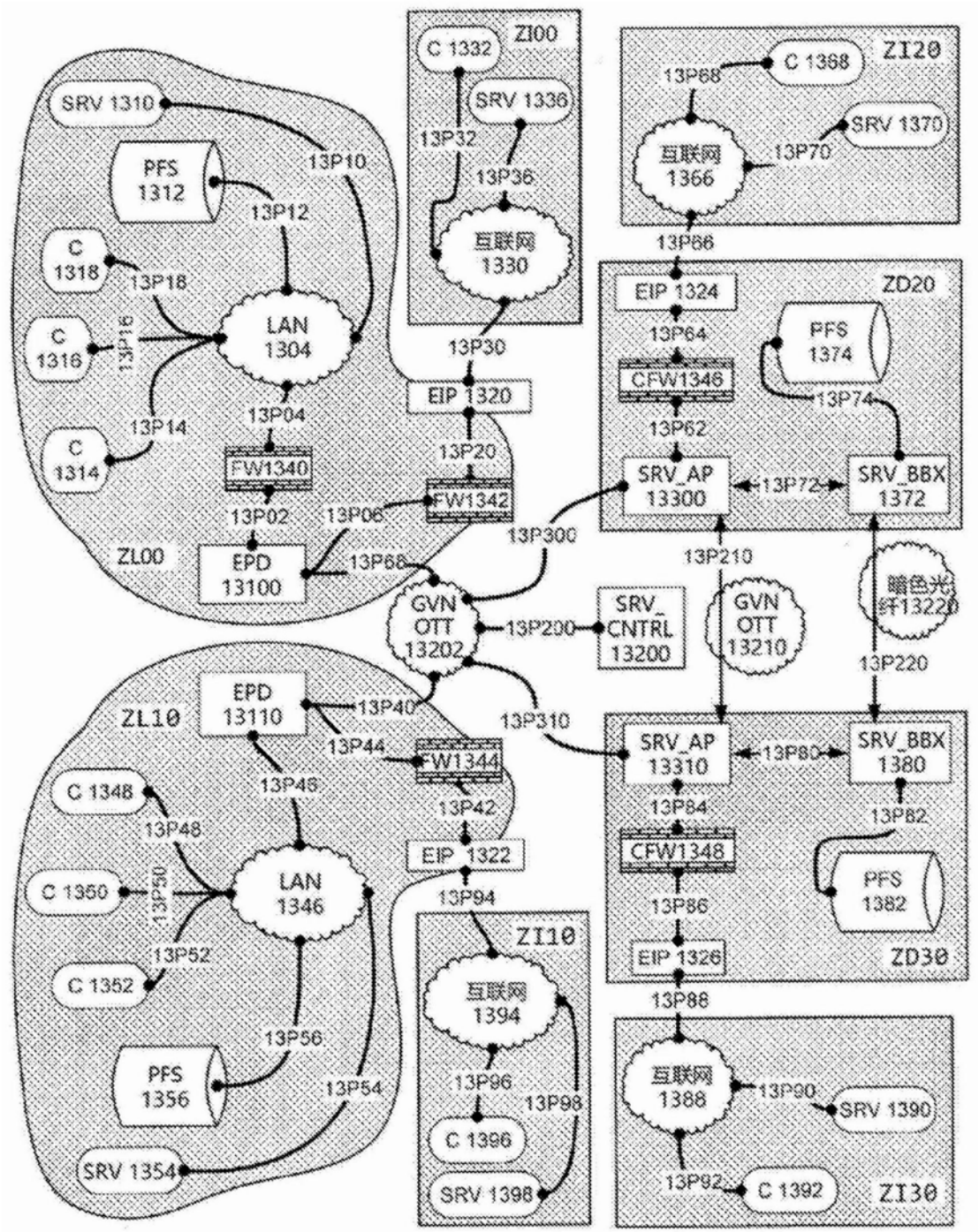

ZI00
C 1332
SRV 1336
13P32
13P36
互联网 1330
13P30
ZI20
13P68
C 1368
SRV 1370
互联网 1366
13P70
13P66
ZD20
EIP 1324
13P64
PFS 1374
CFW1346
13P74
13P62
SRV_AP 13300
13P72
SRV_BBX 1372
13P210
暗色光纤13220
13P220
SRV 1310
13P10
PFS 1312
13P12
C 1318
13P18
C 1316
13P16
LAN 1304
13P14
13P04
C 1314
FW1340
13P02
13P06
FW1342
13P20
EIP 1320
ZL00
EPD 13100
13P08
13P300
GVN OTT 13202
13P200
SRV_ CNTRL 13200
GVN OTT 13210
ZL10
EPD 13110
13P40
13P44
FW1344
13P46
13P42
EIP 1322
13P310
SRV_AP 13310
13P80
SRV_BBX 1380
13P84
13P82
CFW1348
PFS 1382
13P86
EIP 1326
ZD30
C 1348
13P48
C 1350
13P50
LAN 1346
13P52
C 1352
13P56
PFS 1356
13P54
SRV 1354
13P94
ZI10
互联网 1394
13P96
13P98
C 1396
SRV 1398
13P88
互联网 1388
13P90
SRV 1390
13P92
C 1392
ZI30

图13

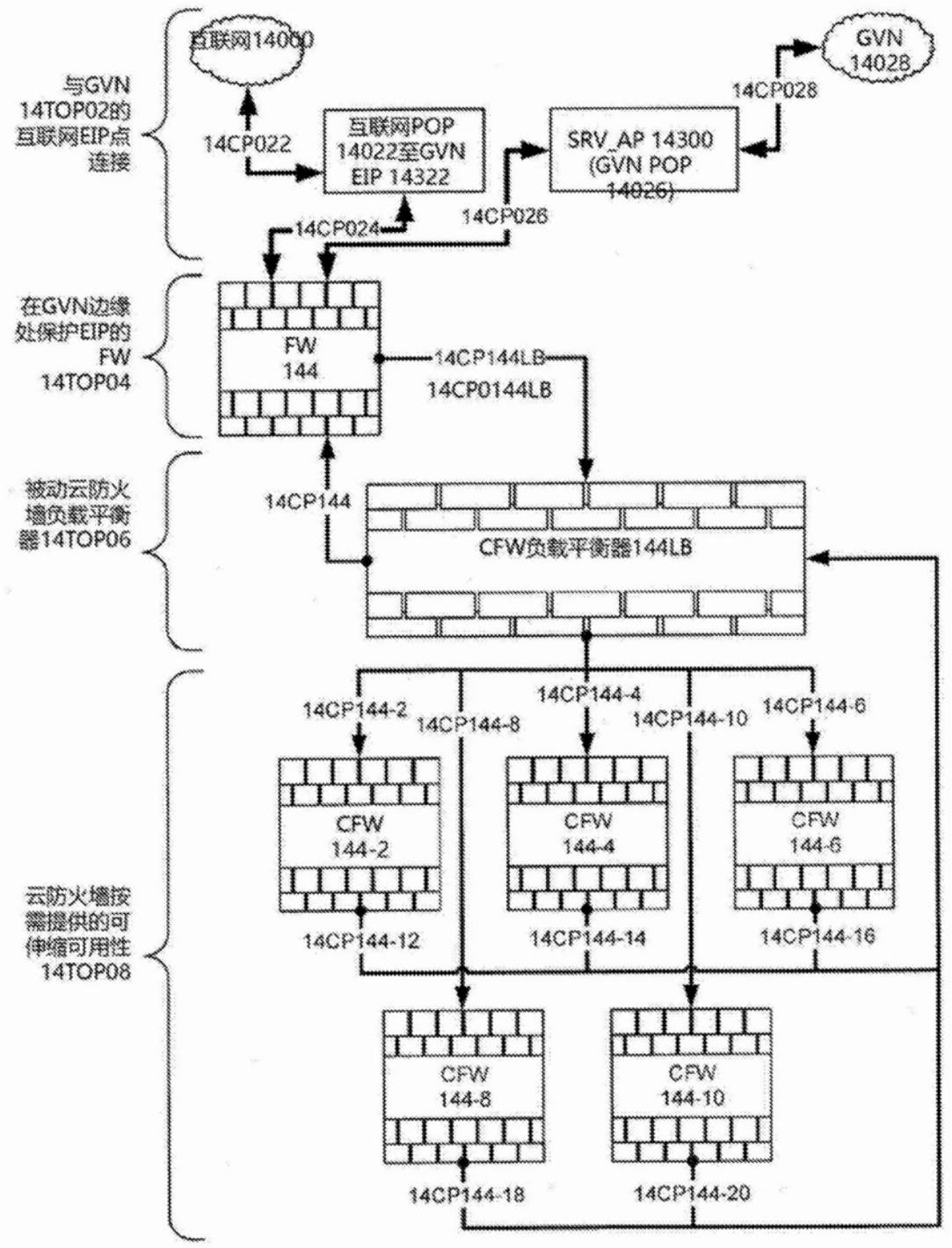

互联网14000
GVN 14028
14CP028
与GVN 14TOP02的互联网EIP点连接
14CP022
互联网POP 14022至GVN EIP 14322
SRV_AP 14300 (GVN POP 14026)
14CP024
14CP026
在GVN边缘处保护EIP的FW 14TOP04
FW 144
14CP144LB
14CP0144LB
被动云防火墙负载平衡器14TOP06
14CP144
CFW负载平衡器144LB
14CP144-2
14CP144-8
14CP144-4
14CP144-10
14CP144-6
CFW 144-2
CFW 144-4
CFW 144-6
14CP144-12
14CP144-14
14CP144-16
云防火墙按需提供的可伸缩可用性 14TOP08
CFW 144-8
CFW 144-10
14CP144-18
14CP144-20

图14

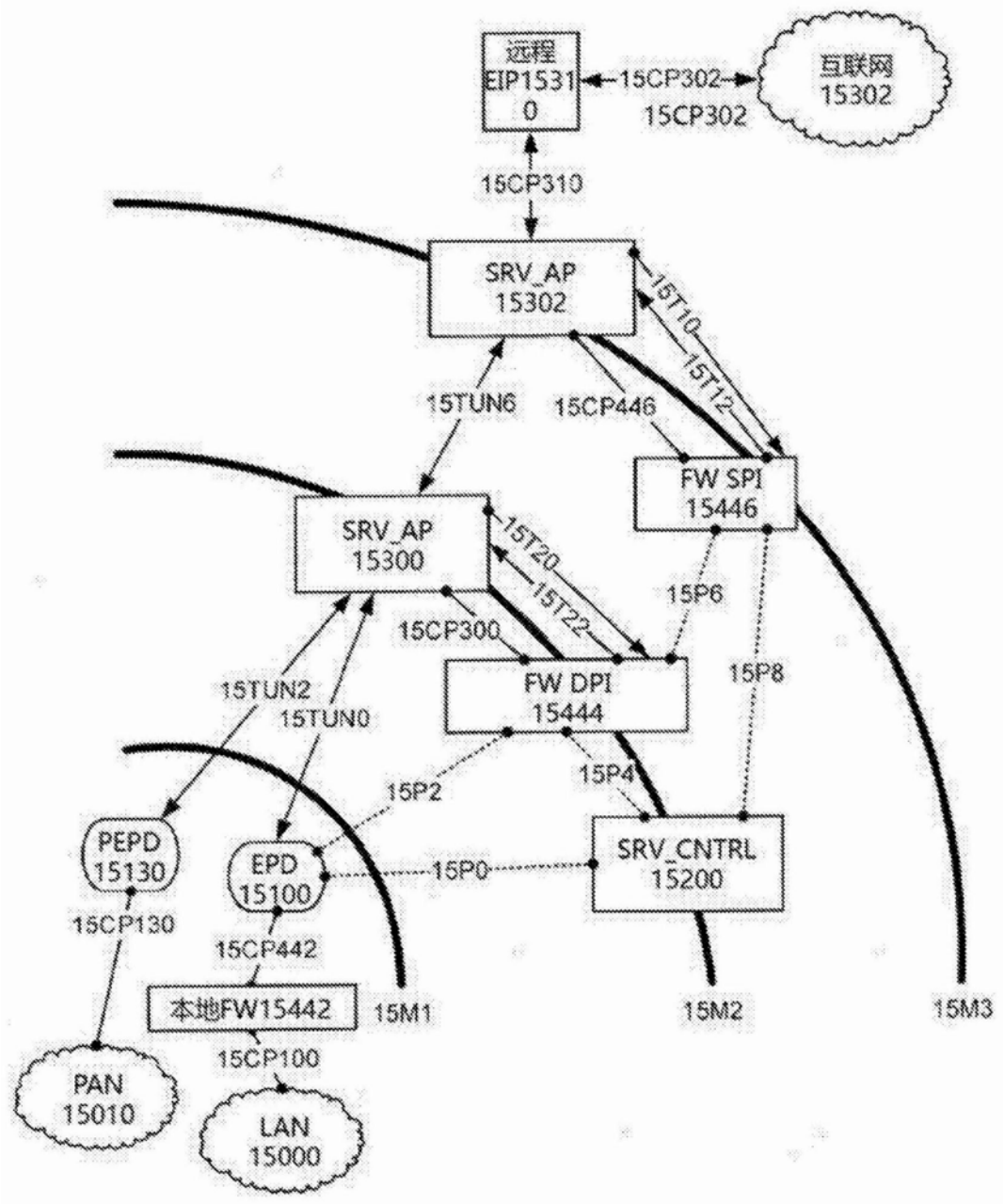

远程
EIP15310
15CP302
互联网
15302
15CP302
15CP310
SRV_AP
15302
15T10
15T12
15TUN6
15CP446
FW SPI
15446
SRV_AP
15300
15T20
15T22
15P6
15CP300
FW DPI
15444
15P8
15TUN2
15TUN0
15P4
15P2
PEPD
15130
EPD
15100
15P0
SRV_CNTRL
15200
15CP130
15CP442
本地FW15442
15M1
15M2
15M3
15CP100
PAN
15010
LAN
15000

图15

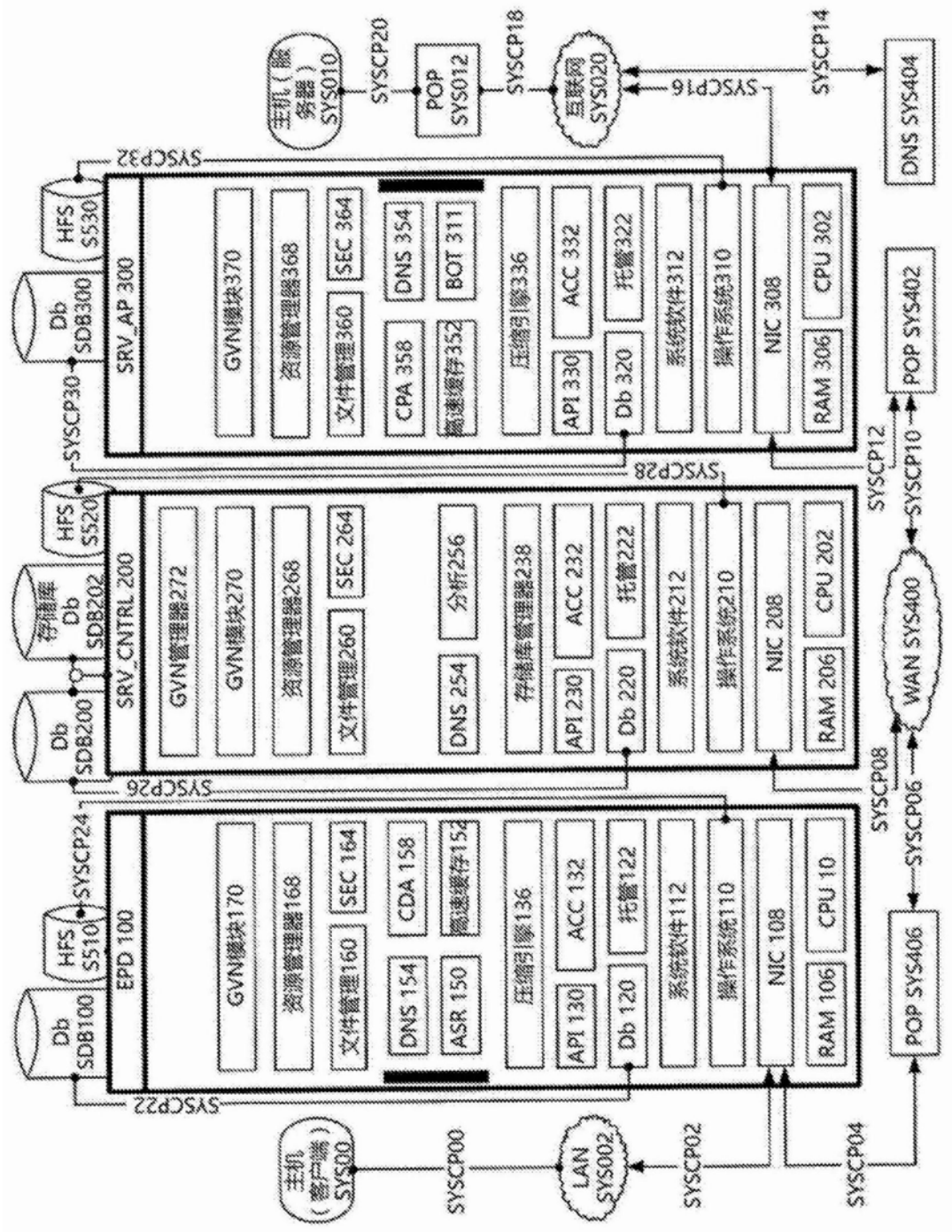

主机（客户端）SYS00
SYSCP00
LAN SYS002
SYSCP02
SYSCP04
SYSCP22
EPD 100
HFS SS10
Db SDB100
SYSCP24
GVN模块170
资源管理器168
文件管理160
SEC 164
CDA 158
高速缓存154
DNS 154
ASR 150
压缩引擎136
API 130
ACC 132
Db 120
托管122
系统软件112
操作系统110
NIC 108
CPU 10
RAM 106
POP SYS406
SYSCP06
SYSCP08
WAN SYS400
SYSCP10
SYSCP12
SYSCP26
SRV_CNTRL 200
HFS SS20
存储库 Db SDB202
Db SDB200
GVN管理器272
GVN模块270
资源管理器268
文件管理260
SEC 264
分析256
DNS 254
存储库管理器238
API 230
ACC 232
Db 220
托管222
系统软件212
操作系统210
NIC 208
CPU 202
RAM 206
POP SYS402
SYSCP28
SYSCP30
SRV_AP 300
HFS SS30
Db SDB300
GVN模块370
资源管理器368
文件管理360
SEC 364
CPA 358
高速缓存352
DNS 354
BOT 311
压缩引擎336
API 330
ACC 332
Db 320
托管322
系统软件312
操作系统310
NIC 308
CPU 302
RAM 306
SYSCP32
主机（服务器）SYS010
SYSCP20
POP SYS012
SYSCP18
互联网 SYS020
SYSCP16
SYSCP14
DNS SYS404

图16

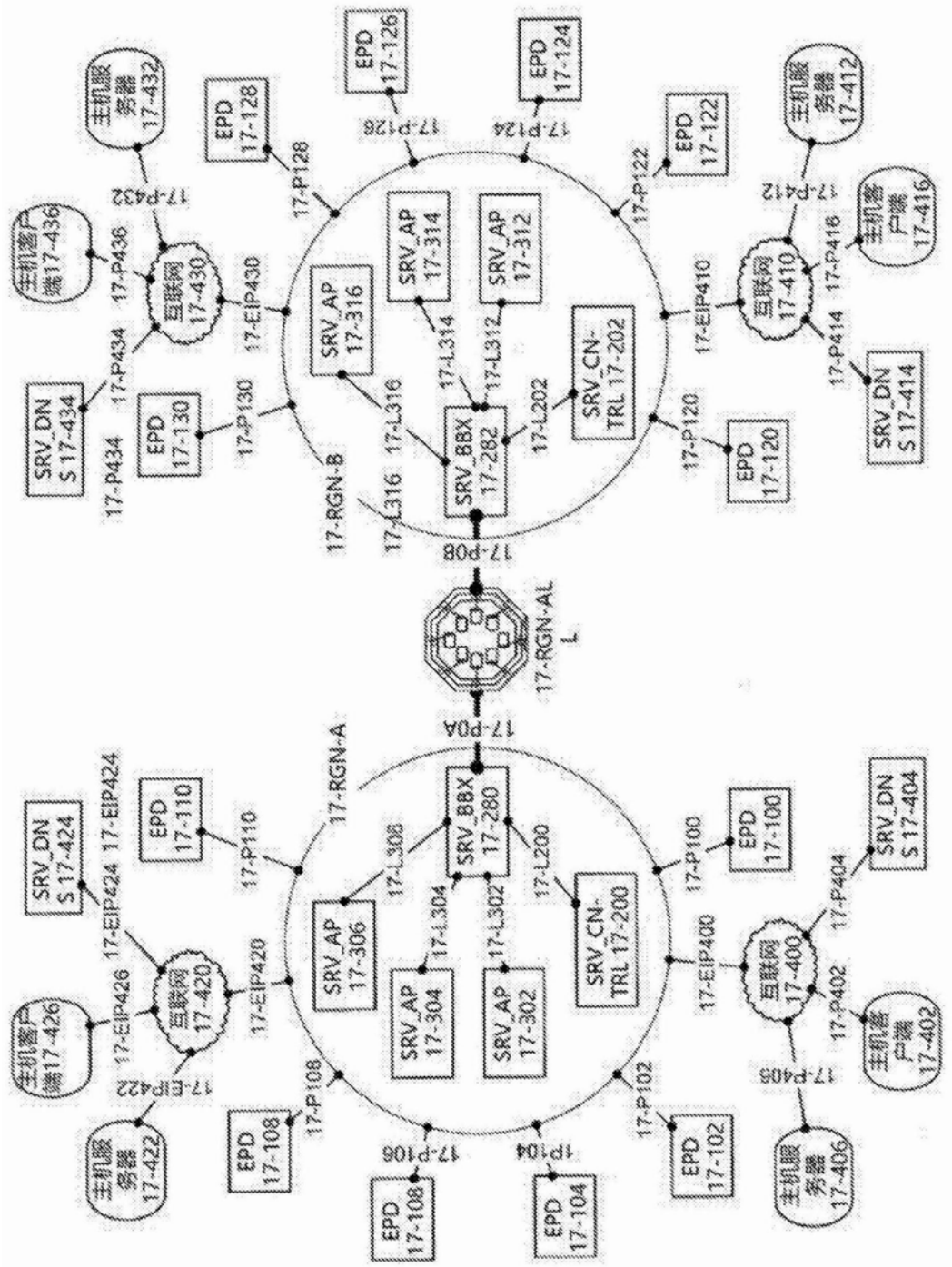

17-RGN-A
17-RGN-B
17-RGN-AL L
17-P08
17-P0A
SRV_BBX 17-282
SRV_BBX 17-280
SRV_CN-TRL 17-202
SRV_CN-TRL 17-200
SRV_AP 17-316
SRV_AP 17-314
SRV_AP 17-312
SRV_AP 17-306
SRV_AP 17-304
SRV_AP 17-302
17-L316
17-L314
17-L312
17-L306
17-L304
17-L302
17-L202
17-L200
17-EIP430
17-EIP410
17-EIP424
17-EIP420
17-EIP400
17-EIP426
17-EIP422
互联网 17-430
互联网 17-410
互联网 17-420
互联网 17-400
17-P436
17-P434
17-P432
17-P416
17-P414
17-P412
17-P404
17-P402
17-P408
17-P130
17-P128
17-P126
17-P124
17-P122
17-P120
17-P110
17-P108
17-P106
17-P104
17-P102
17-P100
主机客户端 17-436
主机客户端 17-426
主机客户端 17-416
主机客户端 17-402
主机服务器 17-432
主机服务器 17-422
主机服务器 17-412
主机服务器 17-406
SRV_DNS 17-434
SRV_DNS 17-424
SRV_DNS 17-414
SRV_DNS 17-404
EPD 17-130
EPD 17-128
EPD 17-126
EPD 17-124
EPD 17-122
EPD 17-120
EPD 17-110
EPD 17-108
EPD 17-108
EPD 17-104
EPD 17-102
EPD 17-100

图17

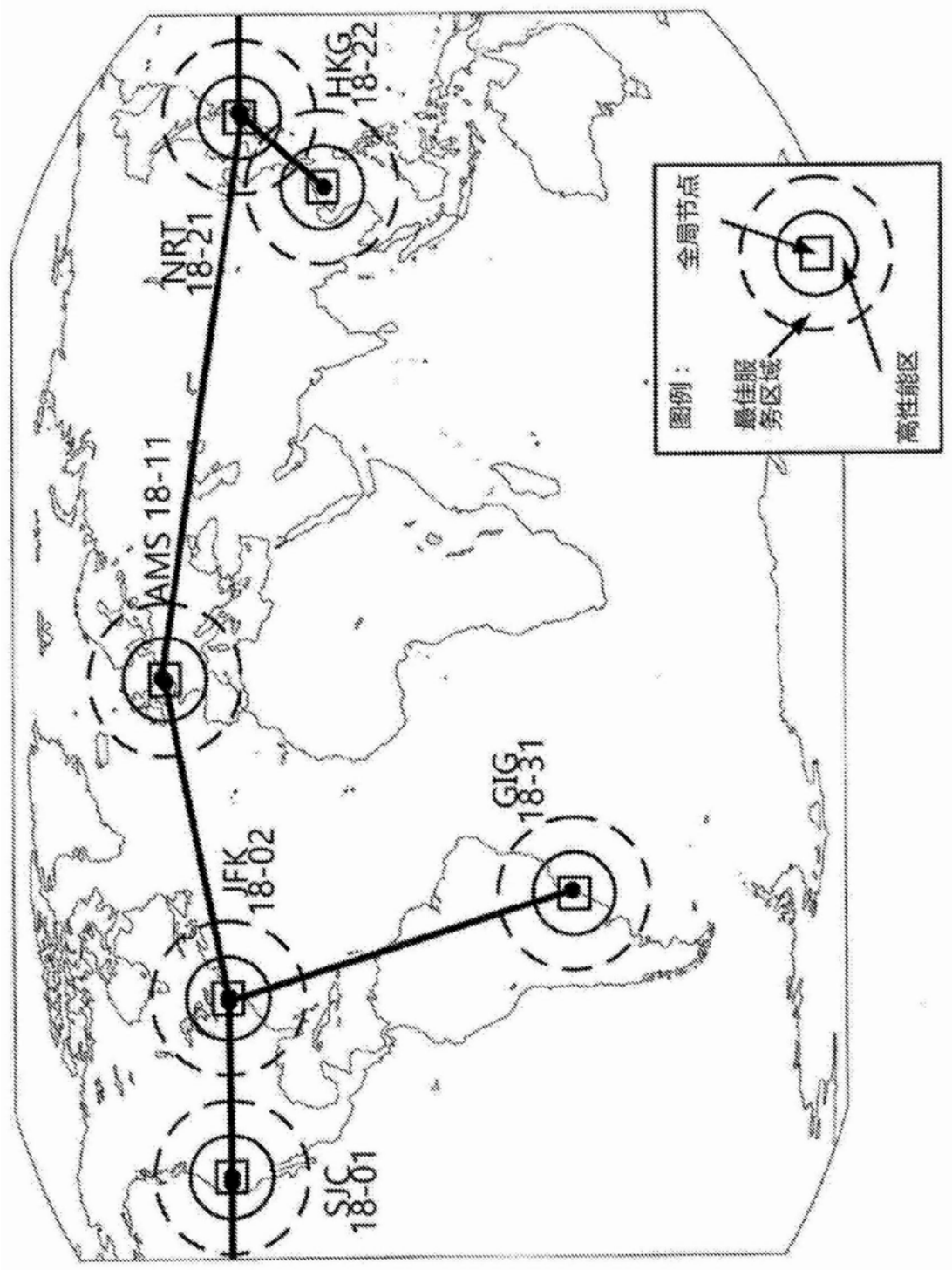

HKG
18-22
NRT
18-21
AMS 18-11
JFK
18-02
GIG
18-31
SJC
18-01
图例：
全局节点
最佳服务区域
高性能区

图18

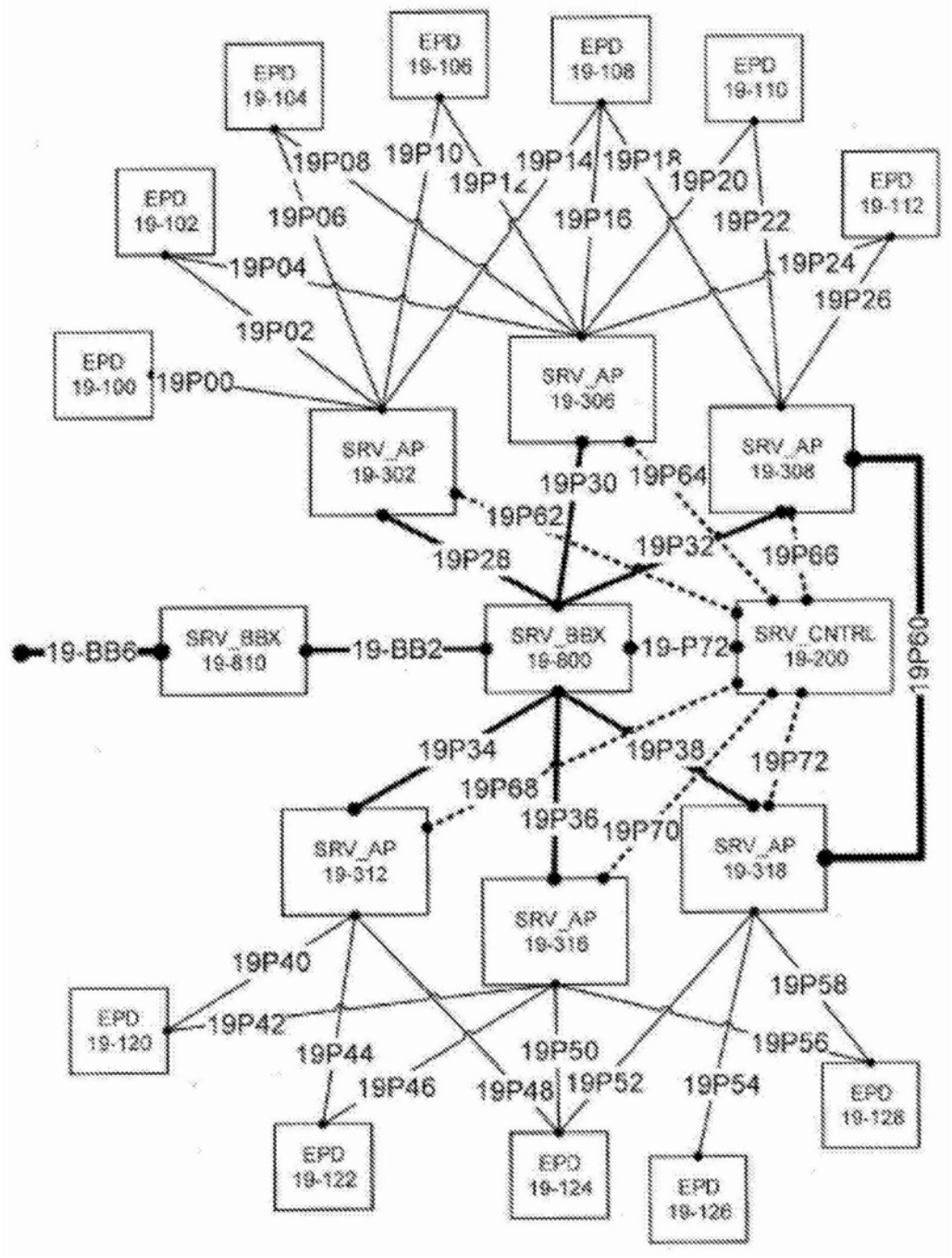

EPD 19-104
EPD 19-106
EPD 19-108
EPD 19-110
EPD 19-102
EPD 19-112
EPD 19-100
SRV_AP 19-306
SRV_AP 19-302
SRV_AP 19-308
SRV_BBX 19-810
SRV_BBX 19-800
SRV_CNTRL 19-200
SRV_AP 19-312
SRV_AP 19-316
SRV_AP 19-318
EPD 19-120
EPD 19-122
EPD 19-124
EPD 19-126
EPD 19-128
19P00
19P02
19P04
19P06
19P08
19P10
19P12
19P14
19P16
19P18
19P20
19P22
19P24
19P26
19P28
19P30
19P32
19P34
19P36
19P38
19P40
19P42
19P44
19P46
19P48
19P50
19P52
19P54
19P56
19P58
19P60
19P62
19P64
19P66
19P68
19P70
19P72
19-BB2
19-BB6
19-P72

图19

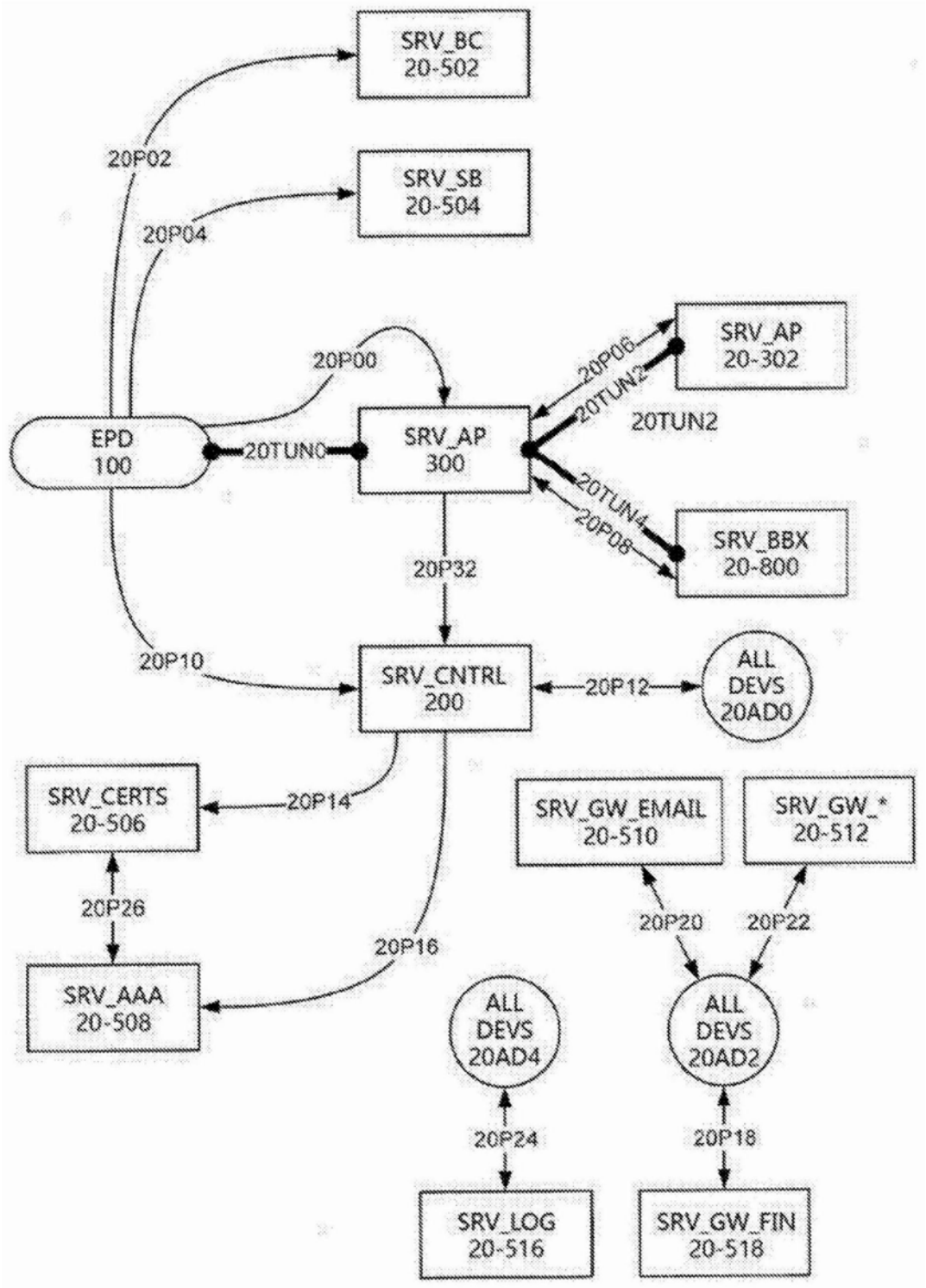

SRV_BC
20-502
20P02
SRV_SB
20-504
20P04
20P00
SRV_AP
20-302
20P06
20TUN2
20TUN2
EPD
100
20TUN0
SRV_AP
300
20TUN4
20P08
SRV_BBX
20-800
20P32
20P10
SRV_CNTRL
200
20P12
ALL
DEVS
20AD0
SRV_CERTS
20-506
20P14
SRV_GW_EMAIL
20-510
SRV_GW_*
20-512
20P26
20P20
20P22
20P16
SRV_AAA
20-508
ALL
DEVS
20AD4
ALL
DEVS
20AD2
20P24
20P18
SRV_LOG
20-516
SRV_GW_FIN
20-518

图20

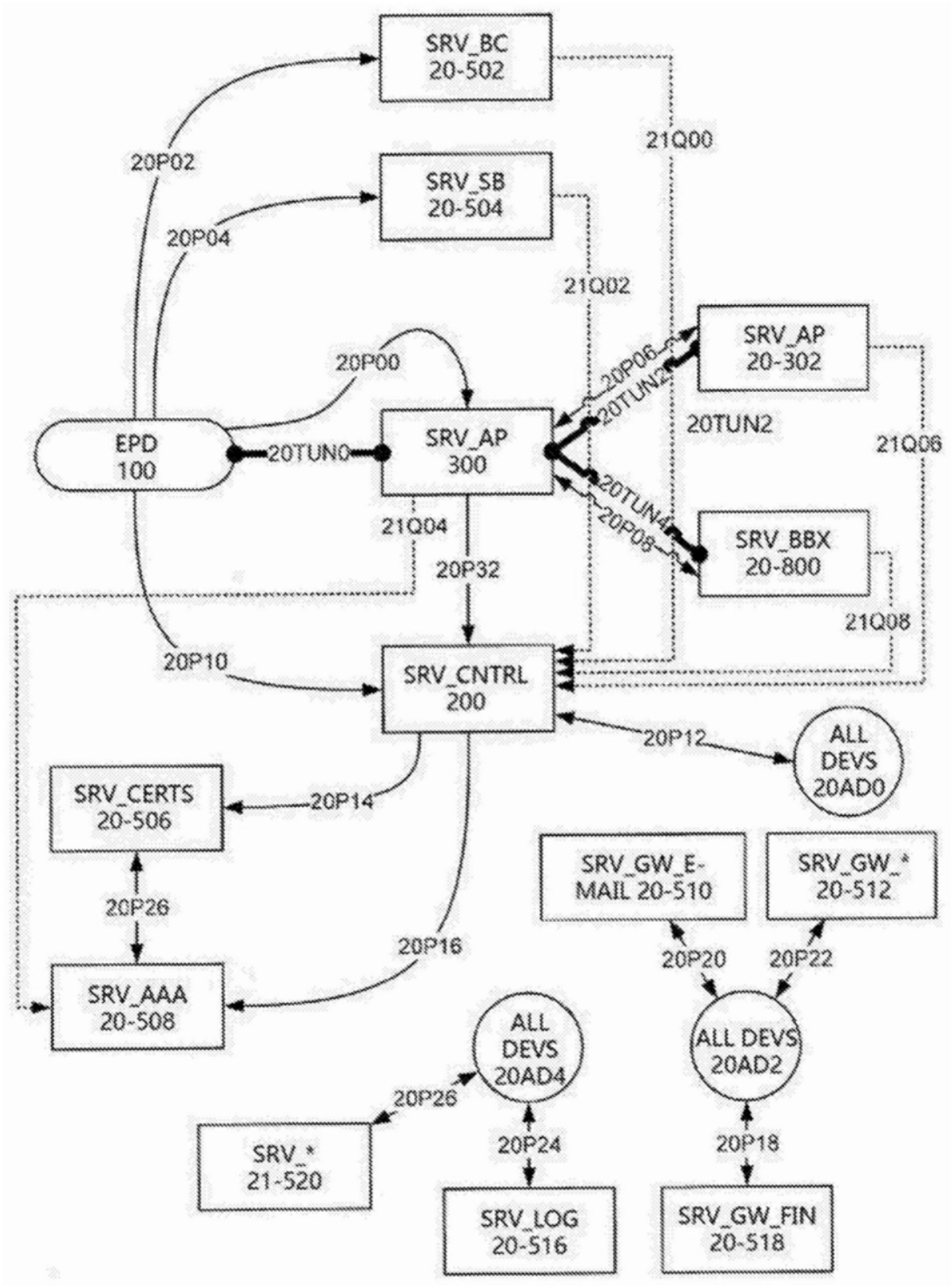

SRV_BC
20-502
SRV_SB
20-504
SRV_AP
20-302
SRV_AP
300
EPD
100
SRV_BBX
20-800
SRV_CNTRL
200
ALL
DEVS
20AD0
SRV_CERTS
20-506
SRV_GW_E-
MAIL 20-510
SRV_GW_*
20-512
SRV_AAA
20-508
ALL
DEVS
20AD4
ALL DEVS
20AD2
SRV_*
21-520
SRV_LOG
20-516
SRV_GW_FIN
20-518
20P02
20P04
20P00
20TUN0
20P06
20TUN2
20TUN4
20P08
20TUN2
21Q00
21Q02
21Q04
21Q06
21Q08
20P32
20P10
20P12
20P14
20P26
20P16
20P20
20P22
20P26
20P24
20P18

图21

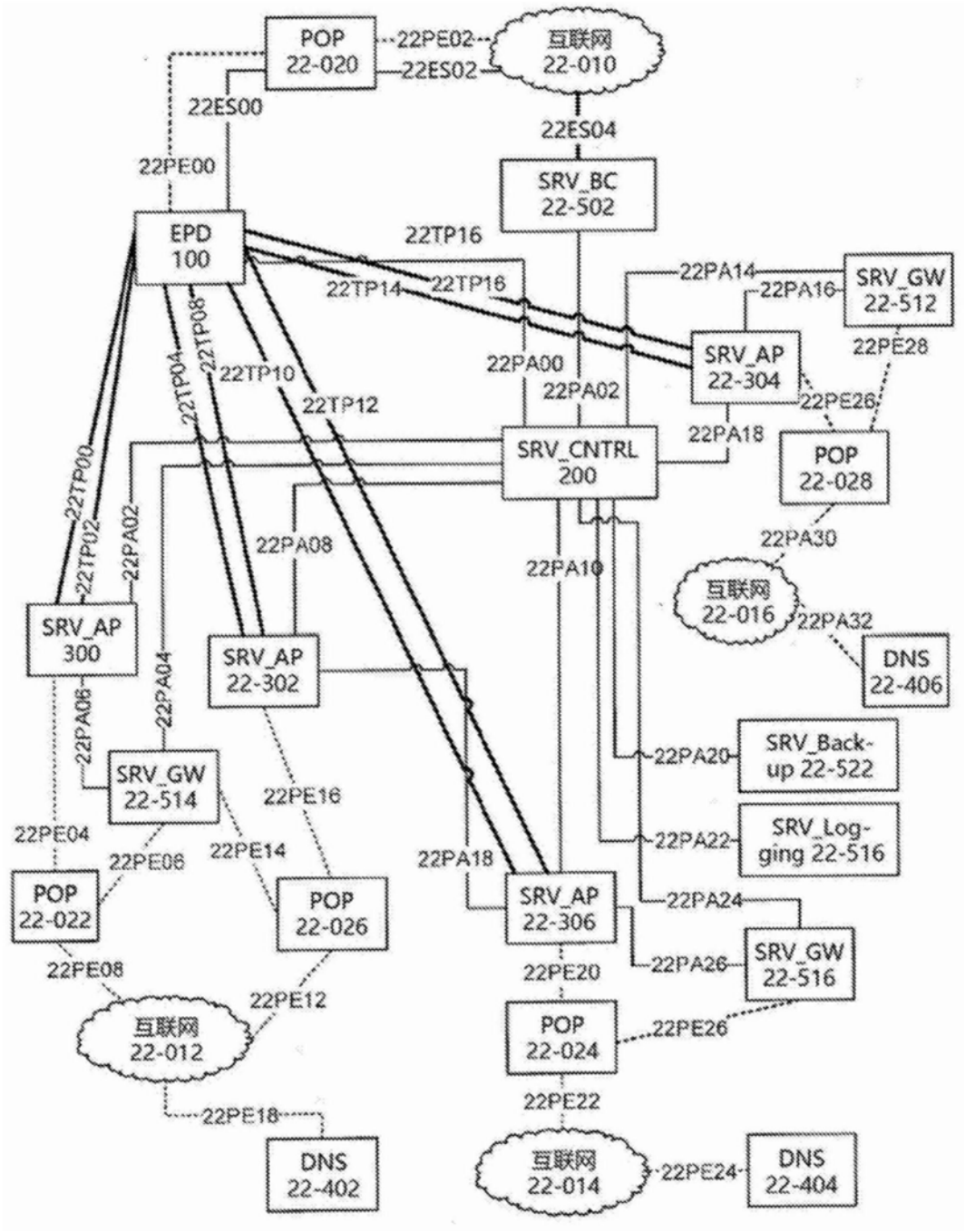

POP
22-020
22PE02
22ES02
互联网
22-010
22ES00
22ES04
22PE00
SRV_BC
22-502
EPD
100
22TP16
22TP14
22TP16
22PA14
22PA16
SRV_GW
22-512
22PE28
SRV_AP
22-304
22PE26
22PA00
22PA02
22TP04
22TP08
22TP10
22TP12
22PA18
SRV_CNTRL
200
POP
22-028
22TP00
22TP02
22PA02
22PA08
22PA10
22PA30
互联网
22-016
22PA32
DNS
22-406
SRV_AP
300
SRV_AP
22-302
22PA04
22PA06
SRV_GW
22-514
22PA20
SRV_Back-
up 22-522
22PE16
22PE04
22PE06
22PE14
22PA18
22PA22
SRV_Log-
ging 22-516
POP
22-022
POP
22-026
SRV_AP
22-306
22PA24
22PA26
SRV_GW
22-516
22PE08
22PE20
22PE12
POP
22-024
22PE26
互联网
22-012
22PE22
22PE18
DNS
22-402
互联网
22-014
22PE24
DNS
22-404

图22

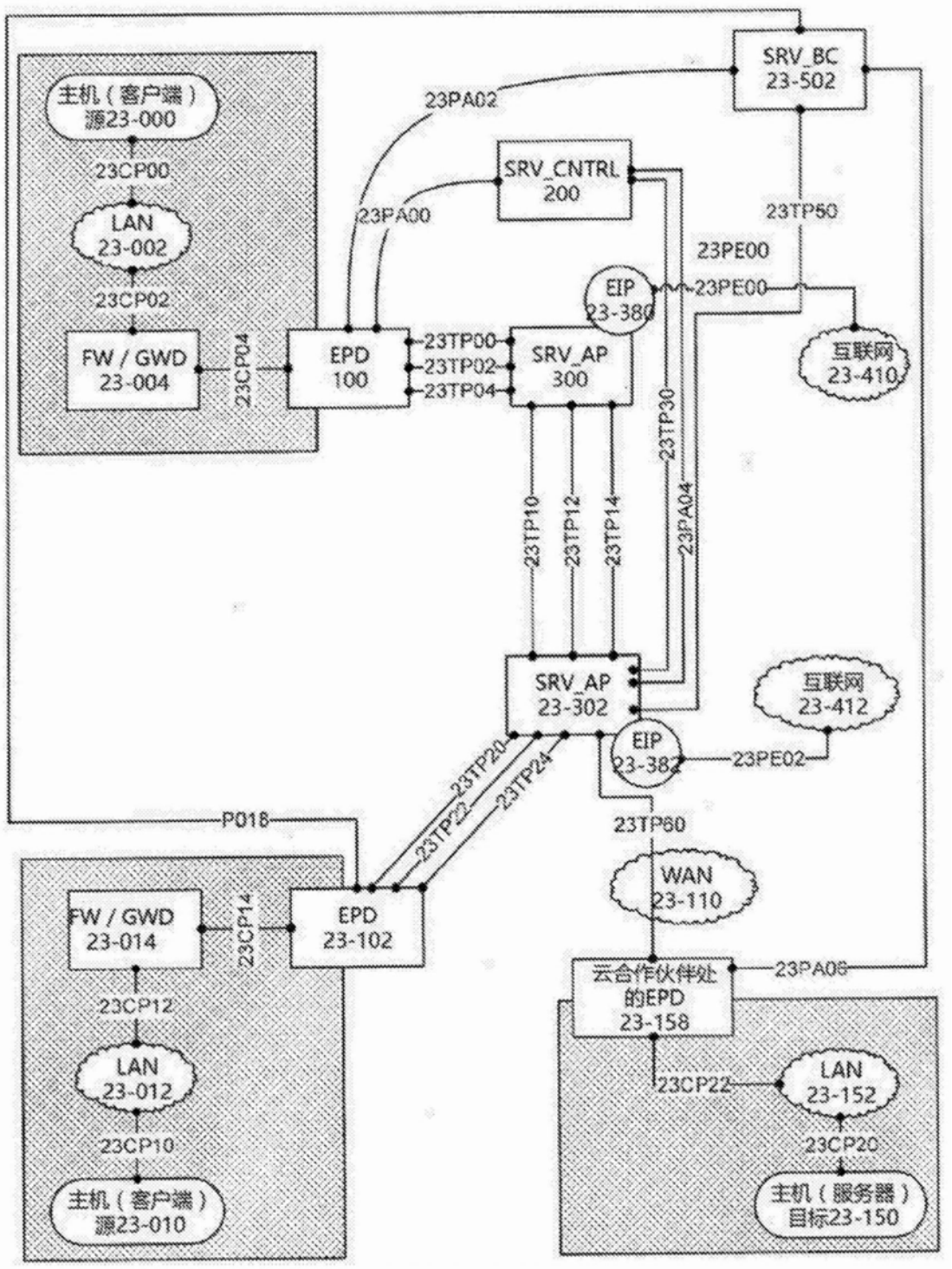

主机（客户端）
源23-000
23CP00
LAN
23-002
23CP02
FW / GWD
23-004
23CP04
EPD
100
23TP00
23TP02
23TP04
SRV_AP
300
SRV_BC
23-502
23PA02
SRV_CNTRL
200
23PA00
23TP50
23PE00
EIP
23-380
23PE00
互联网
23-410
23TP30
23PA04
23TP10
23TP12
23TP14
SRV_AP
23-302
互联网
23-412
EIP
23-382
23PE02
23TP20
23TP22
23TP24
P018
23TP60
WAN
23-110
FW / GWD
23-014
23CP14
EPD
23-102
云合作伙伴处
的EPD
23-158
23PA08
23CP12
LAN
23-012
23CP10
主机（客户端）
源23-010
23CP22
LAN
23-152
23CP20
主机（服务器）
目标23-150

图23

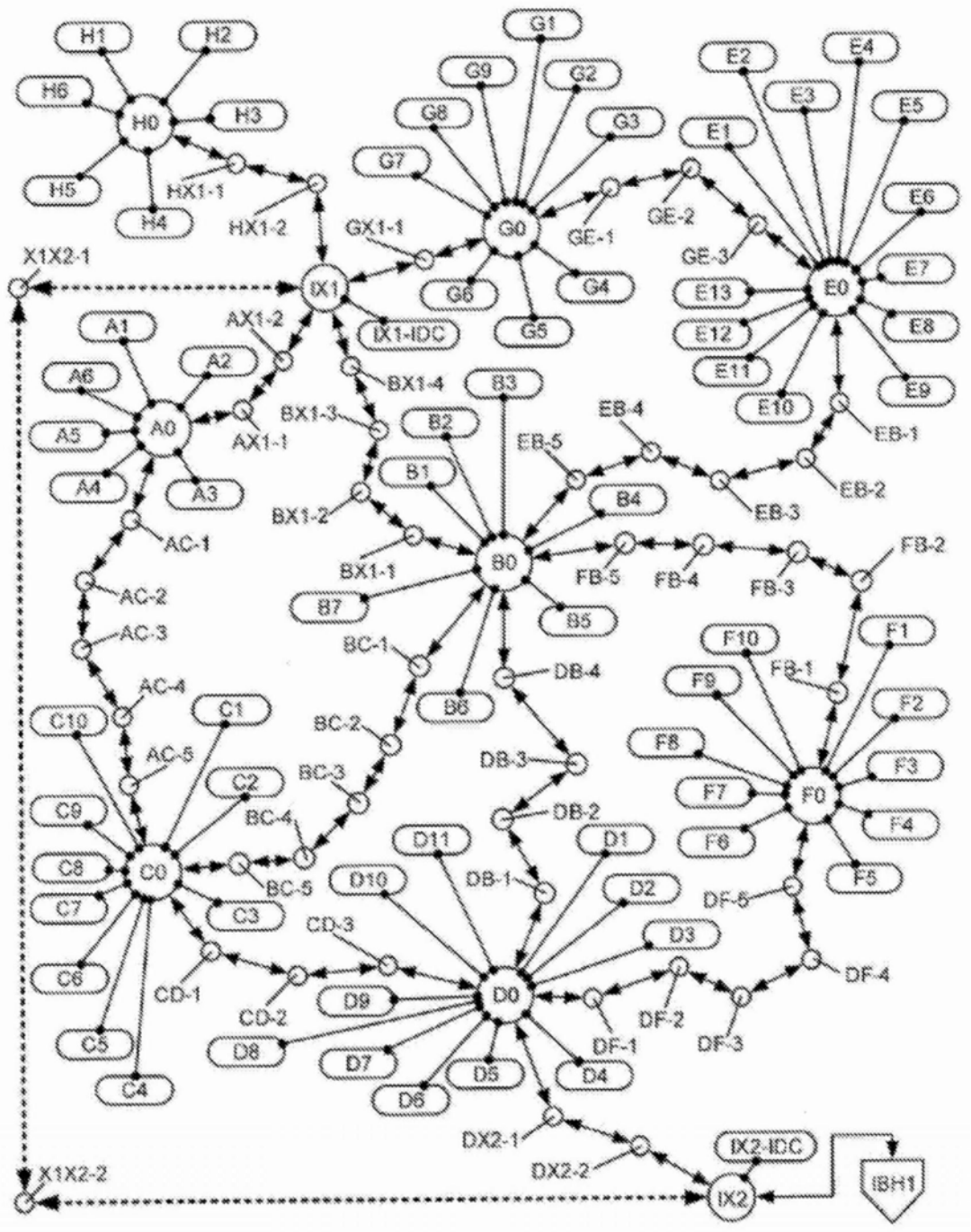

H1
H2
H6
H0
H3
H5
H4
HX1-1
HX1-2
G1
G9
G2
G8
G3
G7
G0
G6
G4
G5
GX1-1
GE-1
GE-2
GE-3
E1
E2
E4
E3
E5
E6
E7
E13
E0
E12
E8
E11
E9
E10
EB-1
EB-2
EB-3
EB-4
EB-5
X1X2-1
IX1
IX1-IDC
AX1-2
AX1-1
A1
A2
A6
A0
A5
A4
A3
BX1-4
BX1-3
BX1-2
BX1-1
B3
B2
B1
B4
B0
B7
B5
B6
FB-1
FB-2
FB-3
FB-4
FB-5
F10
F1
F9
F2
F8
F3
F7
F0
F6
F4
F5
AC-1
AC-2
AC-3
AC-4
AC-5
C10
C1
C2
C9
C8
C0
C7
C3
C6
C5
C4
BC-1
BC-2
BC-3
BC-4
BC-5
DB-4
DB-3
DB-2
DB-1
D11
D1
D10
D2
D3
D0
D9
D8
D7
D6
D5
D4
CD-1
CD-2
CD-3
DF-1
DF-2
DF-3
DF-4
DF-5
DX2-1
DX2-2
IX2-IDC
IX2
IBH1
X1X2-2

图24

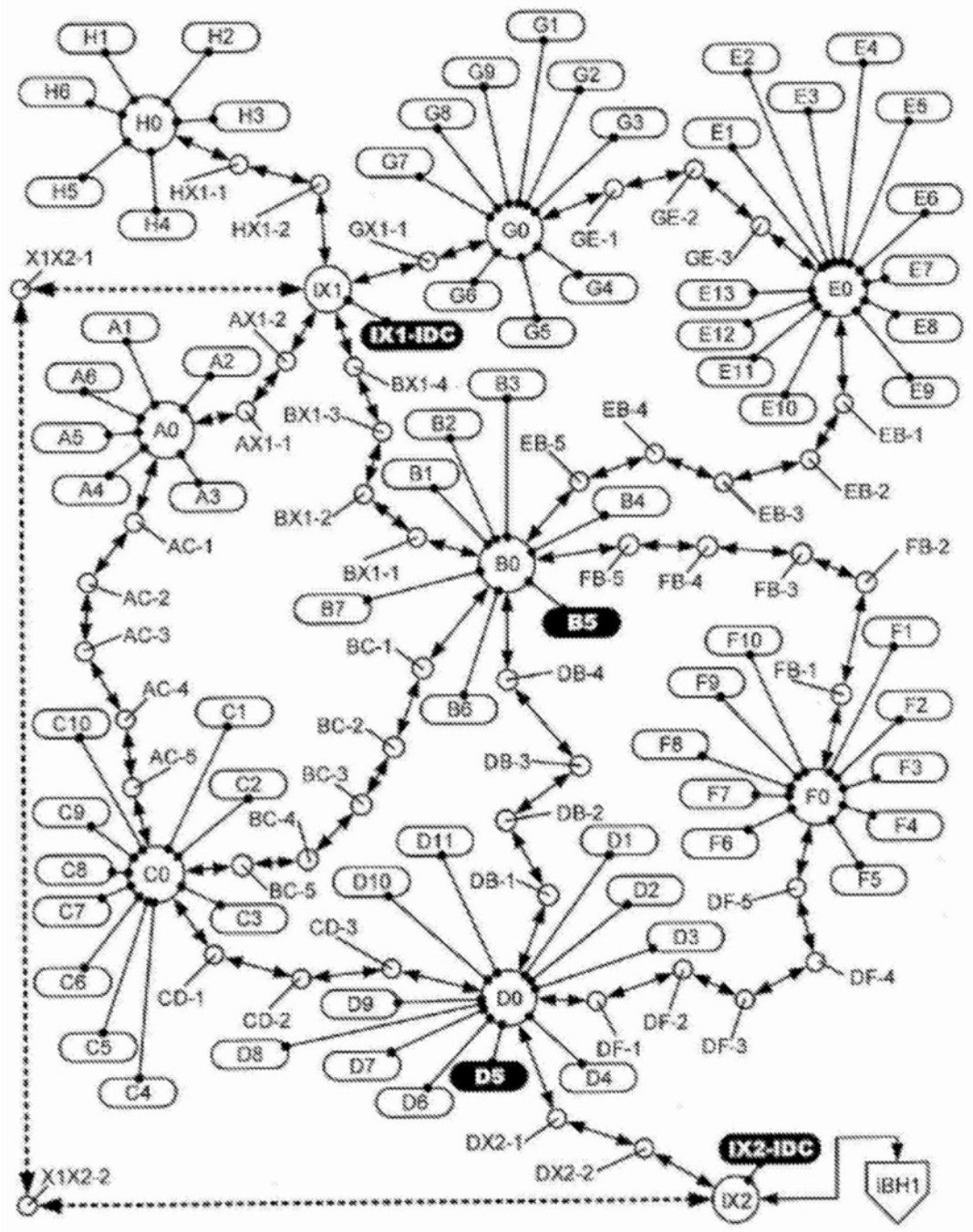

H1
H2
H6
H0
H3
H5
HX1-1
H4
HX1-2
G1
G9
G2
G8
G3
G7
G0
GX1-1
GE-1
GE-2
E2
E4
E3
E5
E1
E6
GE-3
E7
E13
E0
E8
E12
E11
E9
E10
EB-1
EB-2
EB-3
EB-4
EB-5
X1X2-1
IX1
IX1-IDC
G6
G4
G5
A1
AX1-2
A2
A6
A0
AX1-1
A5
A4
A3
AC-1
AC-2
AC-3
AC-4
AC-5
BX1-4
B3
BX1-3
B2
B1
BX1-2
BX1-1
B0
B4
B7
B5
B6
FB-5
FB-4
FB-3
FB-2
FB-1
F10
F1
F9
F2
F8
F3
F7
F0
F4
F6
F5
DF-5
DF-4
DF-3
DF-2
DF-1
BC-1
BC-2
BC-3
BC-4
BC-5
DB-4
DB-3
DB-2
DB-1
C10
C1
C9
C2
C8
C0
C3
C7
C6
C5
C4
CD-3
CD-1
CD-2
D11
D1
D10
D2
D3
D9
D0
D8
D7
D5
D6
D4
DX2-1
DX2-2
IX2-IDC
X1X2-2
IX2
IBH1

图25

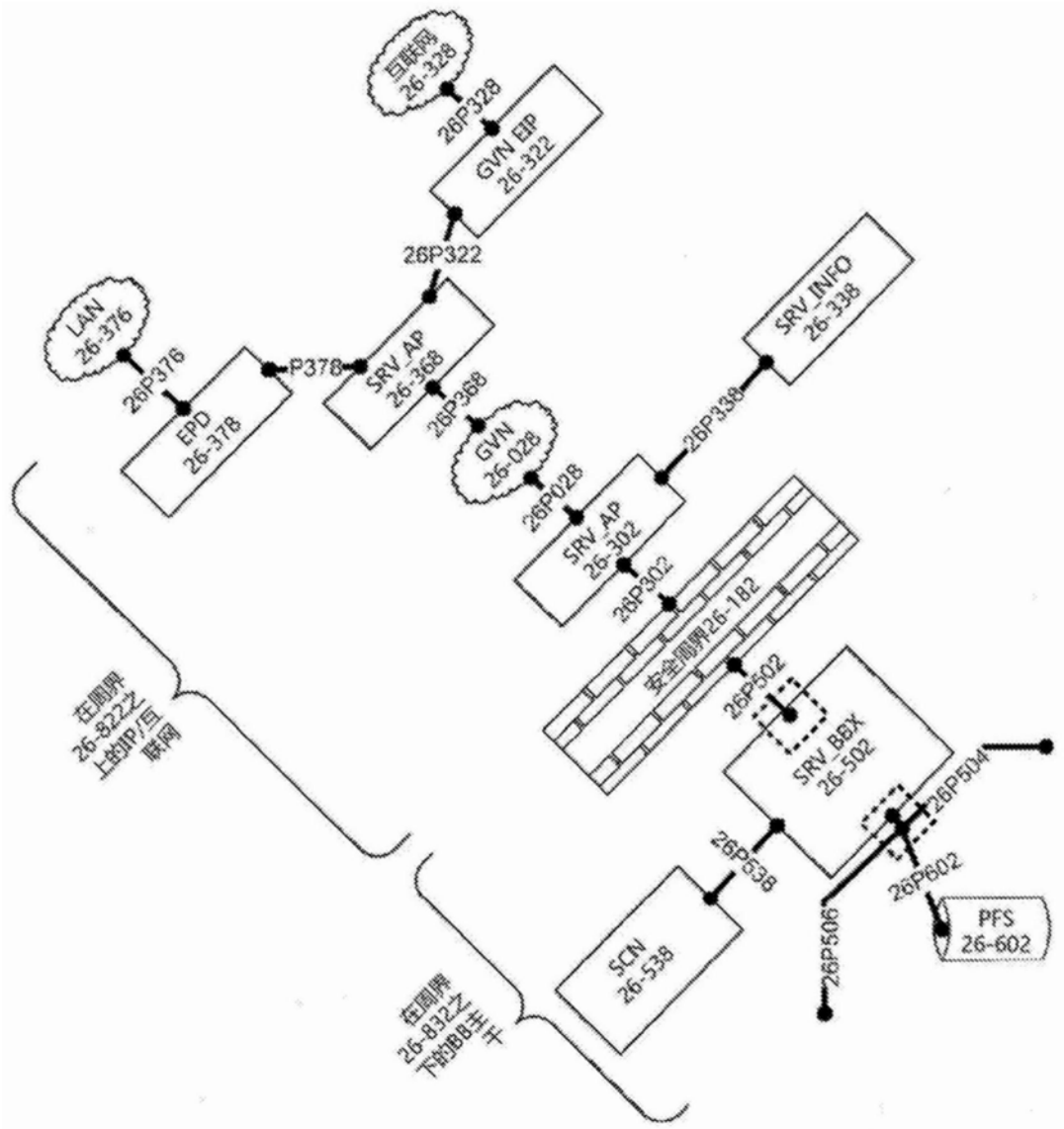

互联网
26-328
26P328
GVN EP
26-322
26P322
LAN
26-376
26P376
EPD
26-378
P378
SRV_AP
26-368
26P368
GVN
26-028
26P028
SRV_INFO
26-338
26P338
SRV_AP
26-302
26P302
安全侧界26-182
26P502
SRV_BBX
26-502
26P504
26P538
SCN
26-538
26P602
26P506
PFS
26-602
在侧界
26-822之
上的IP/互
联网
在侧界
26-832之
下的BB主干

图26

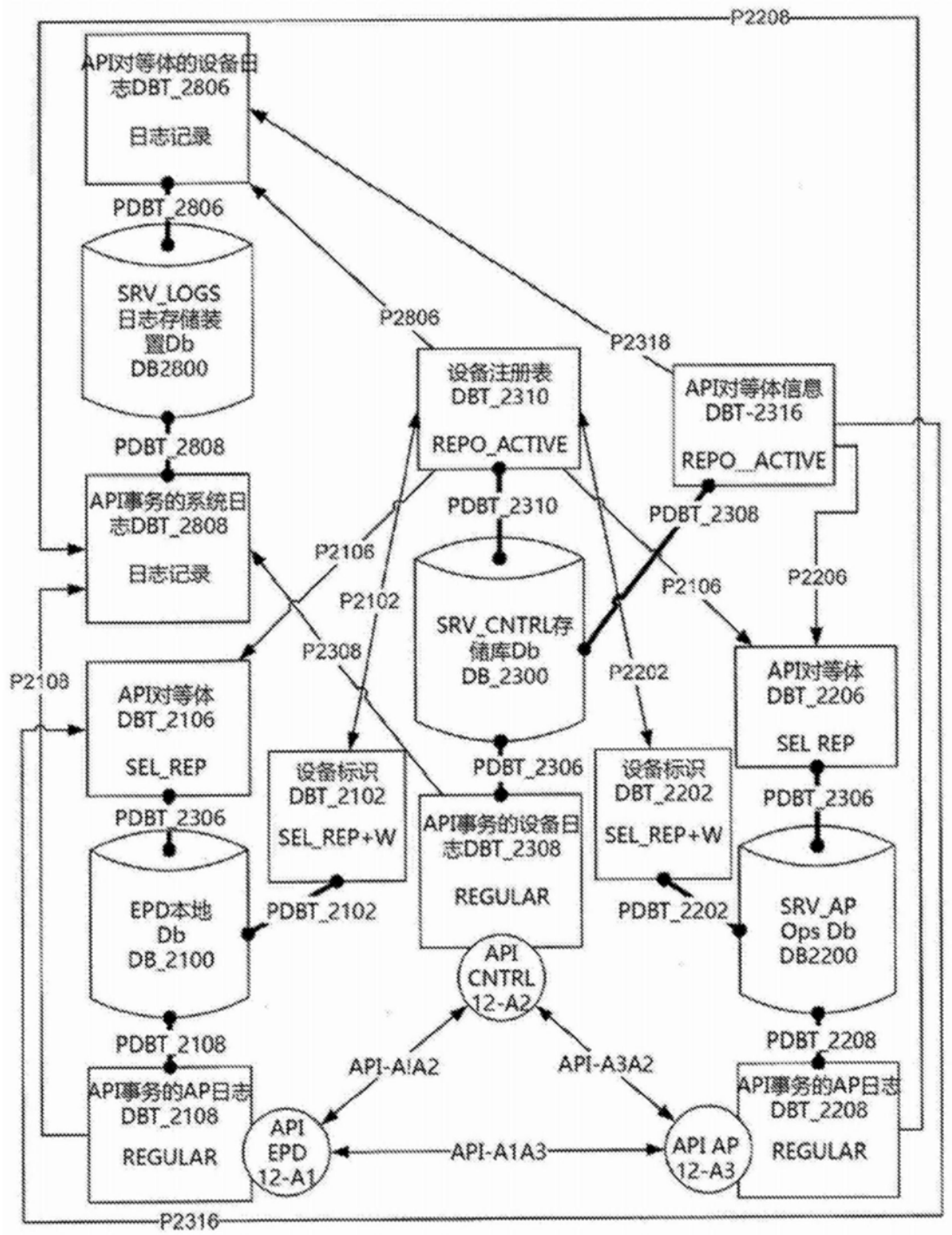

P2208
API对等体的设备日志DBT_2806
日志记录
PDBT_2806
SRV_LOGS
日志存储装置Db
DB2800
PDBT_2808
API事务的系统日志DBT_2808
日志记录
P2806
P2318
设备注册表
DBT_2310
REPO_ACTIVE
API对等体信息
DBT-2316
REPO_ACTIVE
PDBT_2310
PDBT_2308
P2106
P2102
P2308
P2106
P2206
SRV_CNTRL存储库Db
DB_2300
P2108
API对等体
DBT_2106
SEL_REP
P2202
API对等体
DBT_2206
SEL REP
设备标识
DBT_2102
SEL_REP+W
PDBT_2306
设备标识
DBT_2202
SEL_REP+W
PDBT_2306
PDBT_2306
EPD本地
Db
DB_2100
API事务的设备日志DBT_2308
REGULAR
PDBT_2102
PDBT_2202
SRV_AP
Ops Db
DB2200
API
CNTRL
12-A2
PDBT_2108
PDBT_2208
API-A1A2
API-A3A2
API事务的AP日志
DBT_2108
REGULAR
API
EPD
12-A1
API-A1A3
API AP
12-A3
API事务的AP日志
DBT_2208
REGULAR
P2316

图27

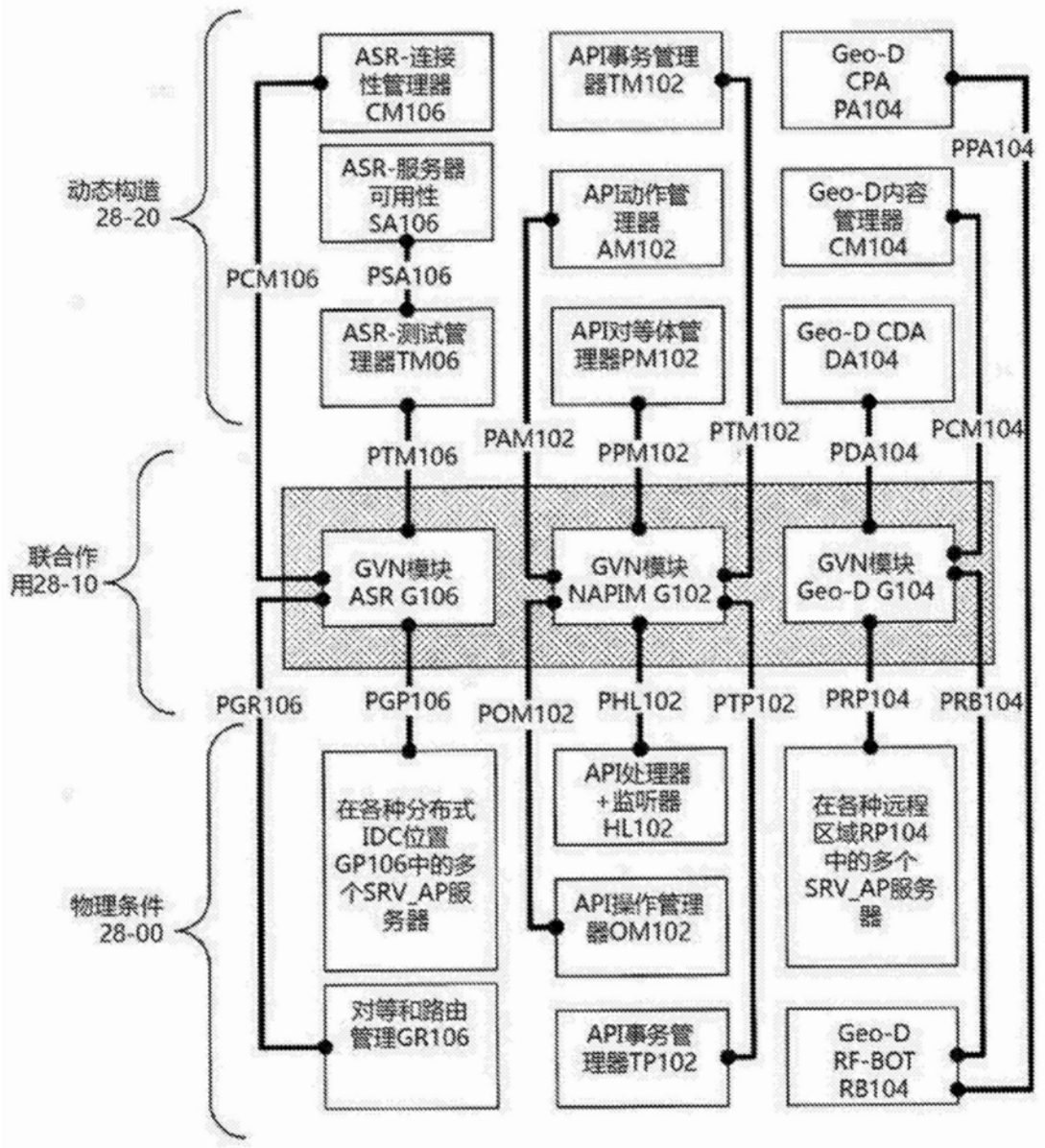

动态构造
28-20
联合作
用28-10
物理条件
28-00
ASR-连接
性管理器
CM106
ASR-服务器
可用性
SA106
ASR-测试管
理器TM06
API事务管理
器TM102
API动作管
理器
AM102
API对等体管
理器PM102
Geo-D
CPA
PA104
Geo-D内容
管理器
CM104
Geo-D CDA
DA104
PPA104
PCM106
PSA106
PTM106
PAM102
PPM102
PTM102
PDA104
PCM104
GVN模块
ASR G106
GVN模块
NAPIM G102
GVN模块
Geo-D G104
PGR106
PGP106
POM102
PHL102
PTP102
PRP104
PRB104
在各种分布式
IDC位置
GP106中的多
个SRV_AP服
务器
API处理器
+监听器
HL102
API操作管理
器OM102
在各种远程
区域RP104
中的多个
SRV_AP服务
器
对等和路由
管理GR106
API事务管
理器TP102
Geo-D
RF-BOT
RB104

图28

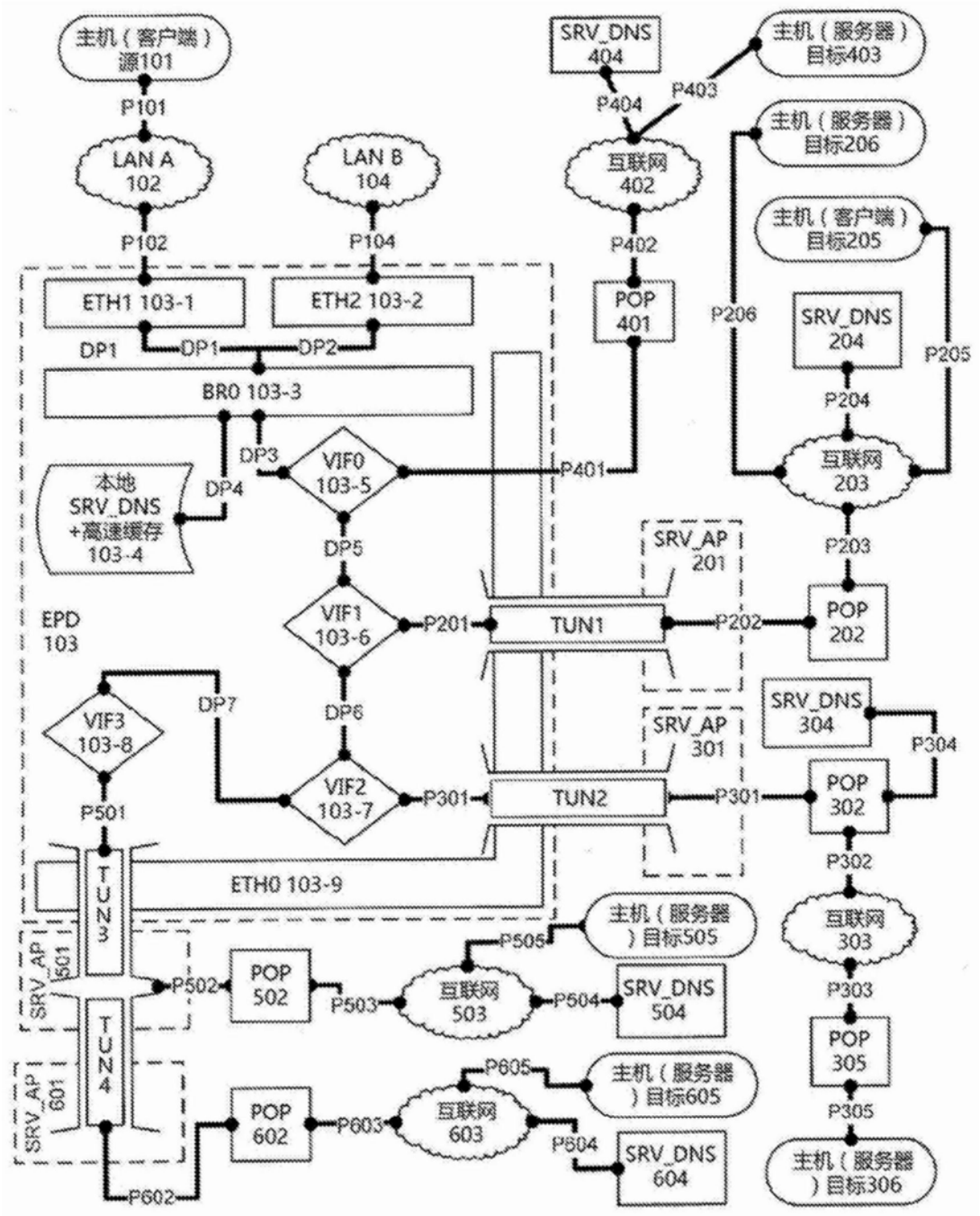

主机（客户端）源101
P101
LAN A 102
LAN B 104
P102
P104
ETH1 103-1
ETH2 103-2
DP1
DP1
DP2
BR0 103-3
DP3
VIF0 103-5
本地 SRV_DNS +高速缓存 103-4
DP4
DP5
EPD 103
VIF1 103-6
P201
TUN1
P202
SRV_AP 201
POP 202
VIF3 103-8
DP7
DP6
VIF2 103-7
P301
TUN2
P301
SRV_AP 301
P501
TUN3
ETH0 103-9
SRV_AP 501
P502
POP 502
P503
互联网 503
P504
SRV_DNS 504
P505
主机（服务器）目标505
TUN4
SRV_AP 601
POP 602
P603
互联网 603
P604
SRV_DNS 604
P605
主机（服务器）目标605
P602
SRV_DNS 404
P404
P403
主机（服务器）目标403
互联网 402
P402
POP 401
P401
主机（服务器）目标206
主机（客户端）目标205
P206
SRV_DNS 204
P205
P204
互联网 203
P203
SRV_DNS 304
P304
POP 302
P302
互联网 303
P303
POP 305
P305
主机（服务器）目标306

图29

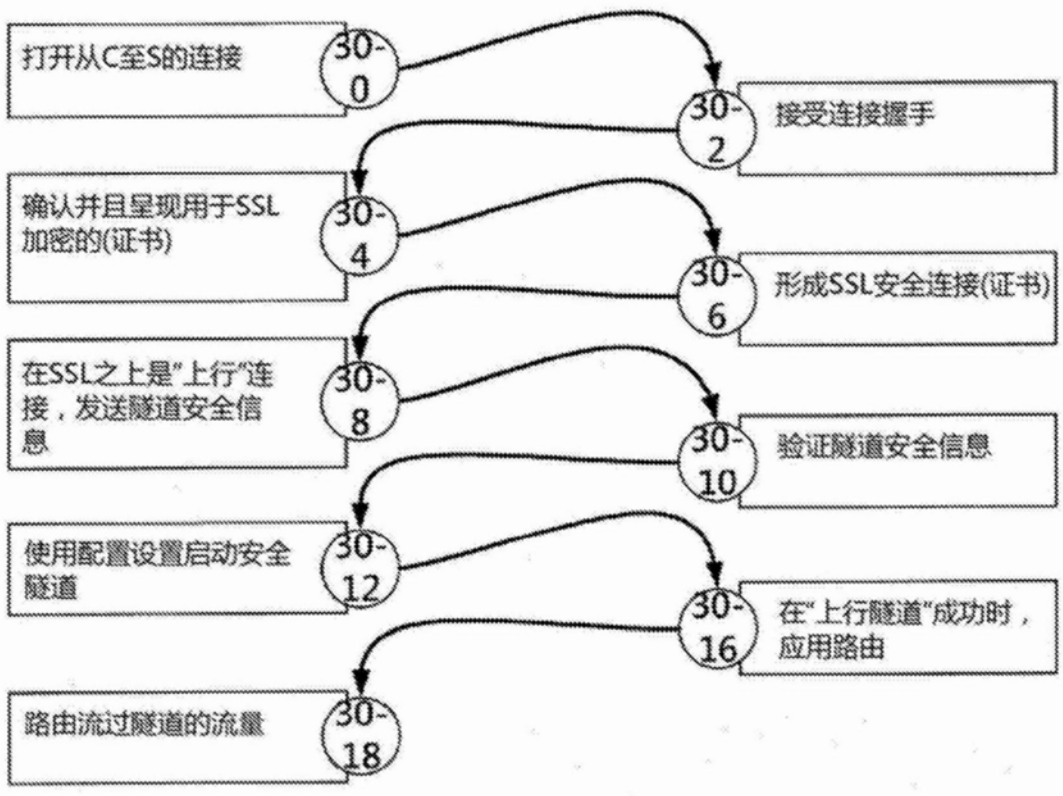

打开从C至S的连接
30-0
接受连接握手
30-2
确认并且呈现用于SSL加密的(证书)
30-4
形成SSL安全连接(证书)
30-6
在SSL之上是"上行"连接，发送隧道安全信息
30-8
验证隧道安全信息
30-10
使用配置设置启动安全隧道
30-12
在"上行隧道"成功时，应用路由
30-16
路由流过隧道的流量
30-18

图30

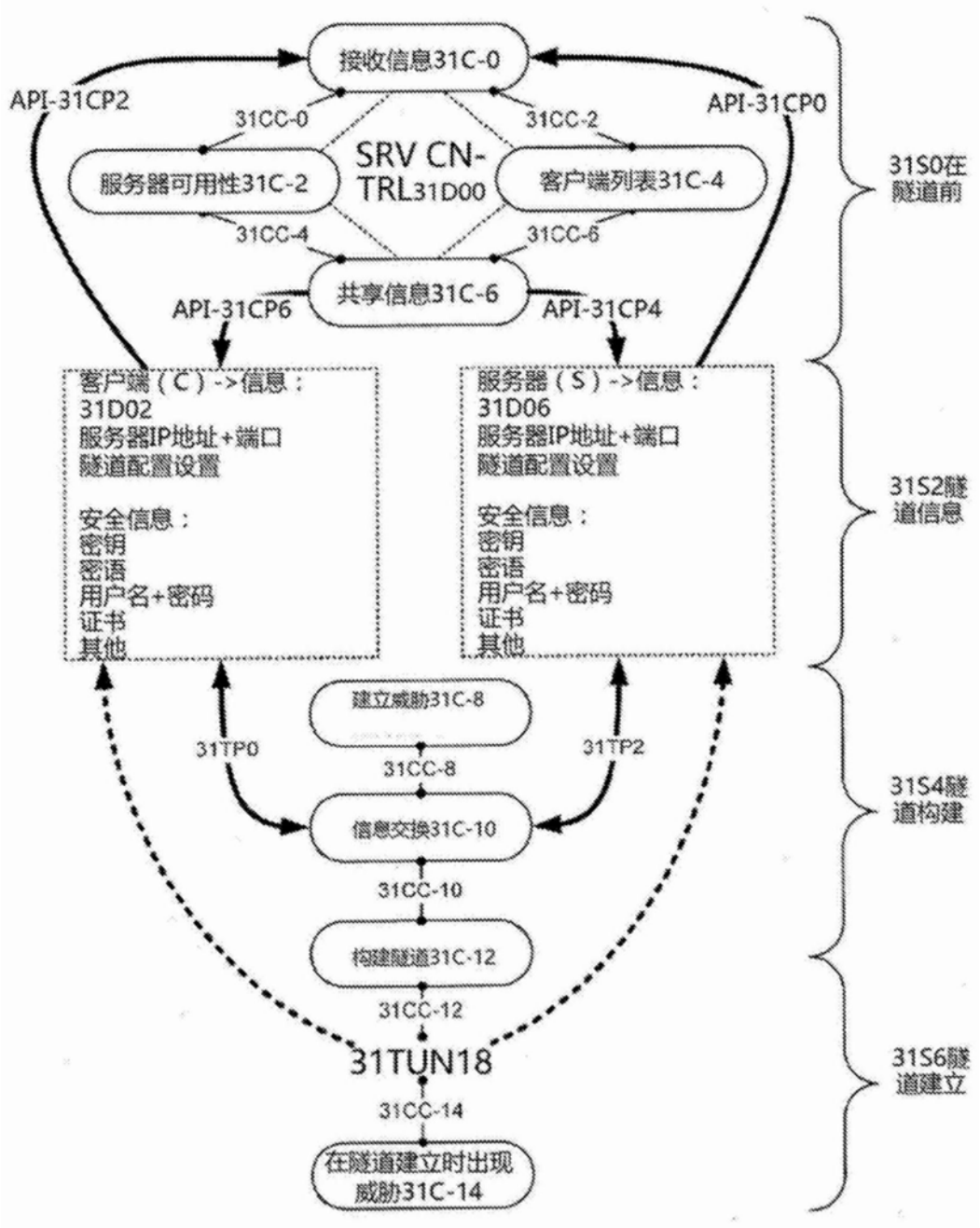

接收信息31C-0
API-31CP2
API-31CP0
31CC-0
31CC-2
服务器可用性31C-2
SRV CN-TRL31D00
客户端列表31C-4
31CC-4
31CC-6
共享信息31C-6
API-31CP6
API-31CP4
客户端（C）->信息：
31D02
服务器IP地址+端口
隧道配置设置
安全信息：
密钥
密语
用户名+密码
证书
其他
服务器（S）->信息：
31D06
服务器IP地址+端口
隧道配置设置
安全信息：
密钥
密语
用户名+密码
证书
其他
建立威胁31C-8
31TP0
31TP2
31CC-8
信息交换31C-10
31CC-10
构建隧道31C-12
31CC-12
31TUN18
31CC-14
在隧道建立时出现威胁31C-14
31S0在隧道前
31S2隧道信息
31S4隧道构建
31S6隧道建立

图31

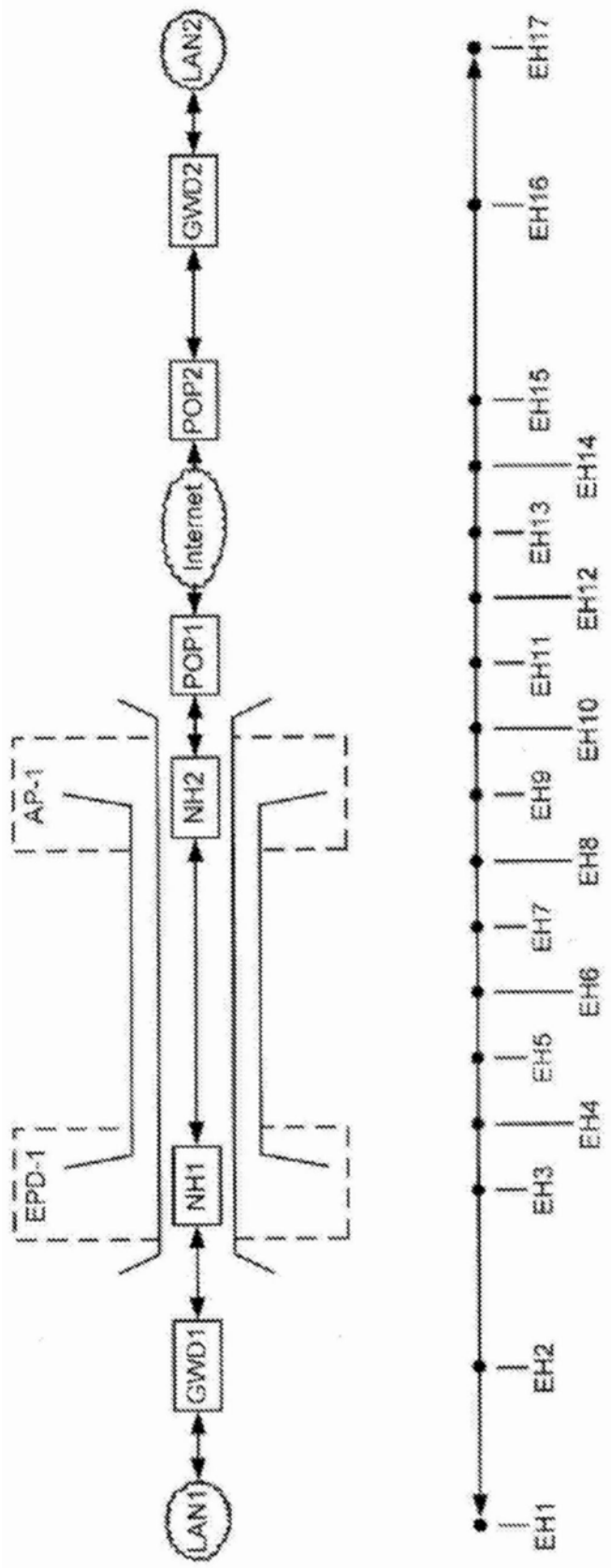

LAN2
GWD2
POP2
Internet
POP1
NH2
NH1
GWD1
LAN1
AP-1
EPD-1
EH1
EH2
EH3
EH4
EH5
EH6
EH7
EH8
EH9
EH10
EH11
EH12
EH13
EH14
EH15
EH16
EH17

图32

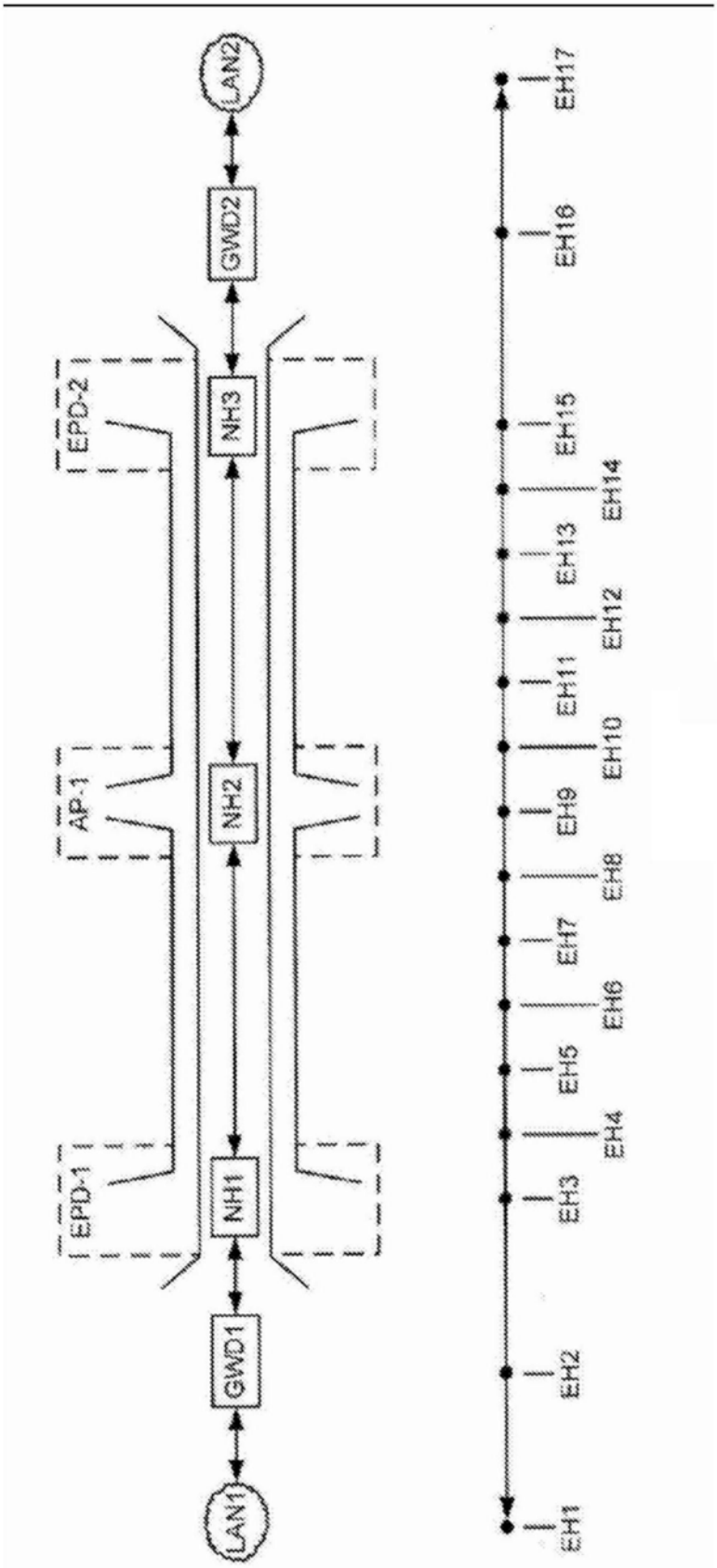

LAN2
GWD2
NH3
NH2
NH1
GWD1
LAN1
EPD-2
AP-1
EPD-1
EH17
EH16
EH15
EH14
EH13
EH12
EH11
EH10
EH9
EH8
EH7
EH6
EH5
EH4
EH3
EH2
EH1

图33

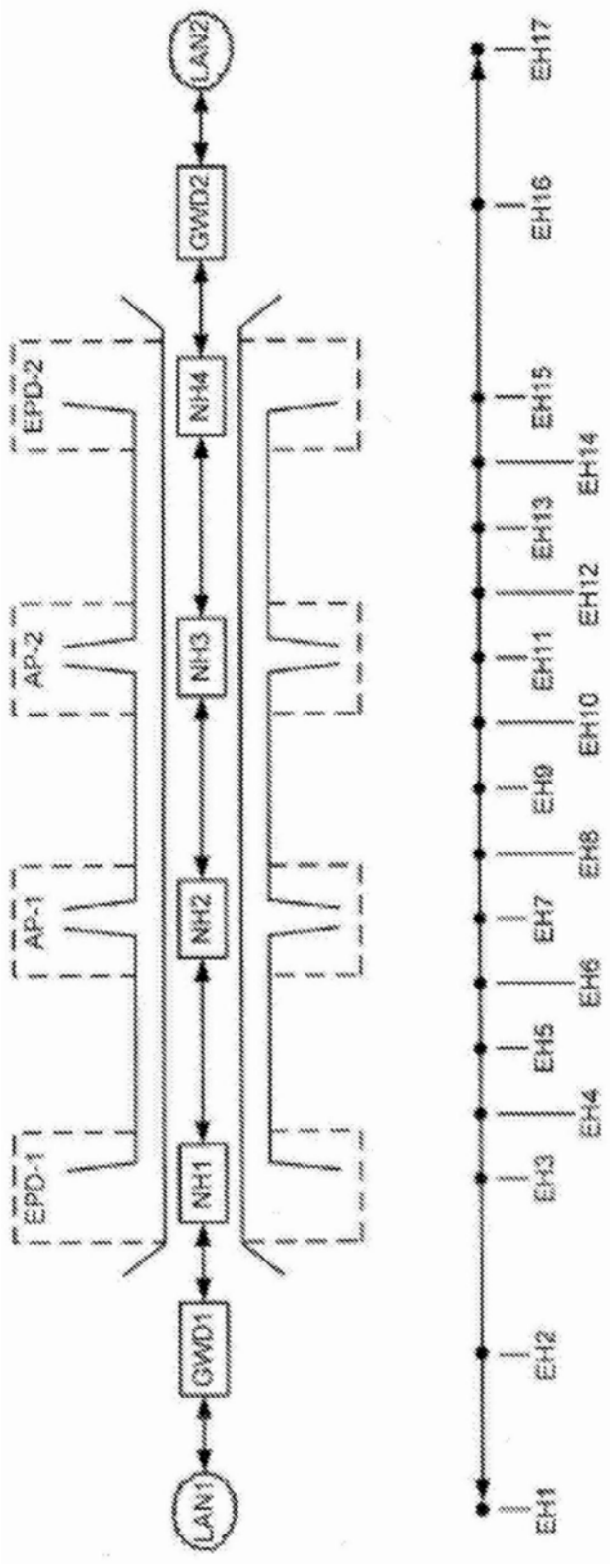

LAN2
GWD2
NH4
NH3
NH2
NH1
GWD1
LAN1
EPD-2
AP-2
AP-1
EPD-1
EH17
EH16
EH15
EH14
EH13
EH12
EH11
EH10
EH9
EH8
EH7
EH6
EH5
EH4
EH3
EH2
EH1

图34

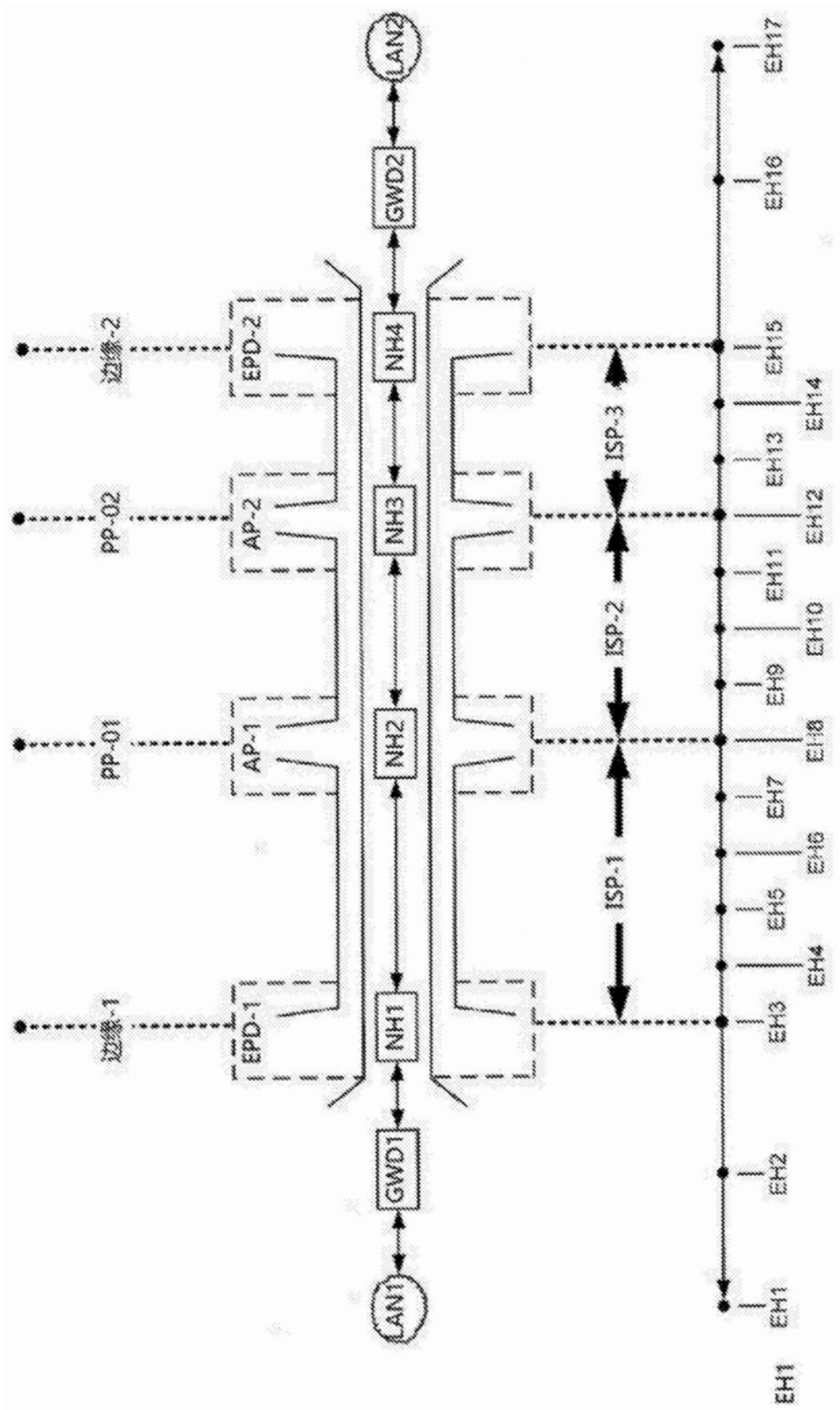

LAN2
GWD2
NH4
NH3
NH2
NH1
GWD1
LAN1
边缘-2
PP-02
PP-01
边缘-1
EPD-2
AP-2
AP-1
EPD-1
ISP-3
ISP-2
ISP-1
EH17
EH16
EH15
EH14
EH13
EH12
EH11
EH10
EH9
EH8
EH7
EH6
EH5
EH4
EH3
EH2
EH1
EH1

图35

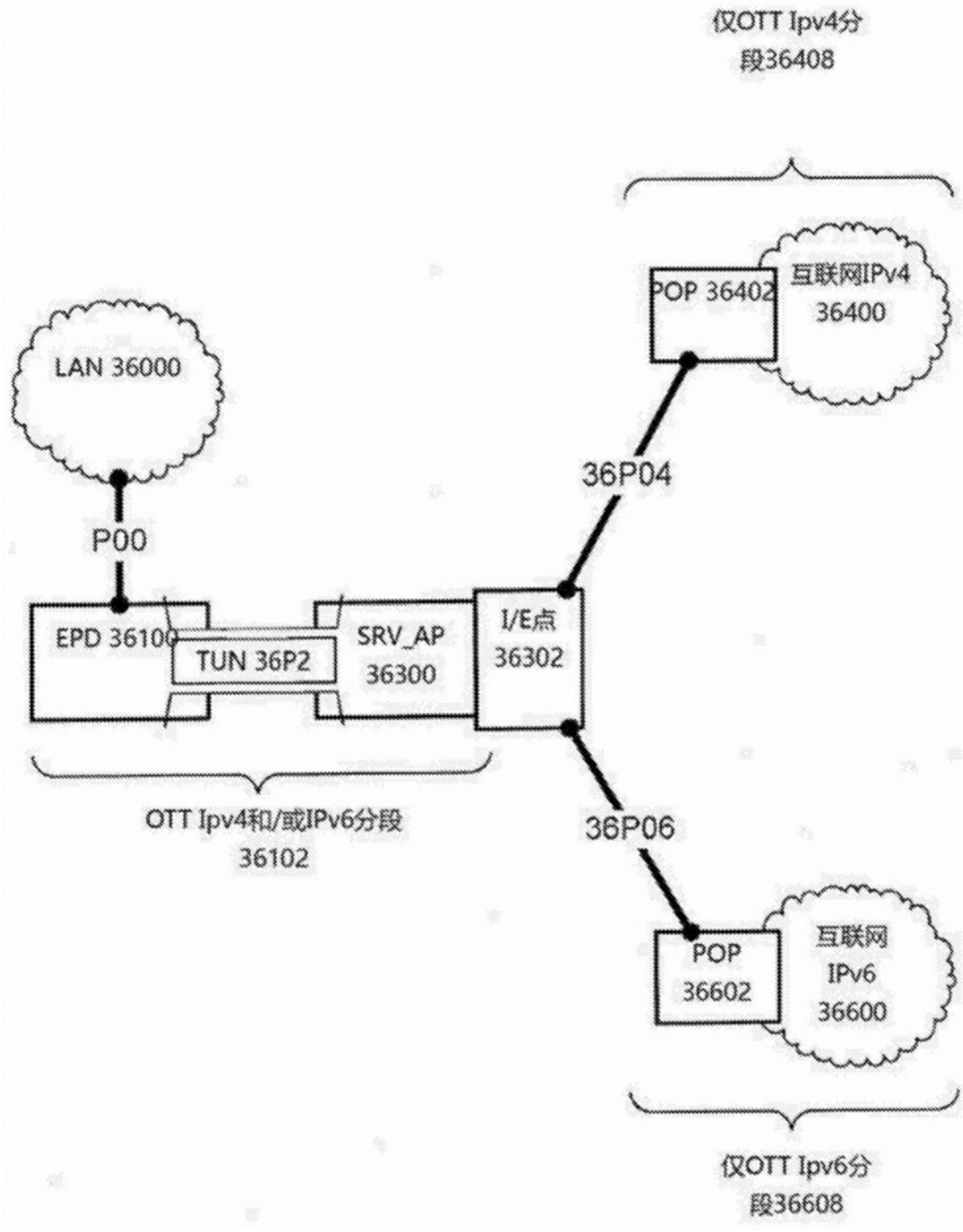

仅OTT Ipv4分
段36408
POP 36402
互联网IPv4
36400
LAN 36000
36P04
P00
EPD 36100
TUN 36P2
SRV_AP
36300
I/E点
36302
OTT Ipv4和/或IPv6分段
36102
36P06
POP
36602
互联网
IPv6
36600
仅OTT Ipv6分
段36608

图36

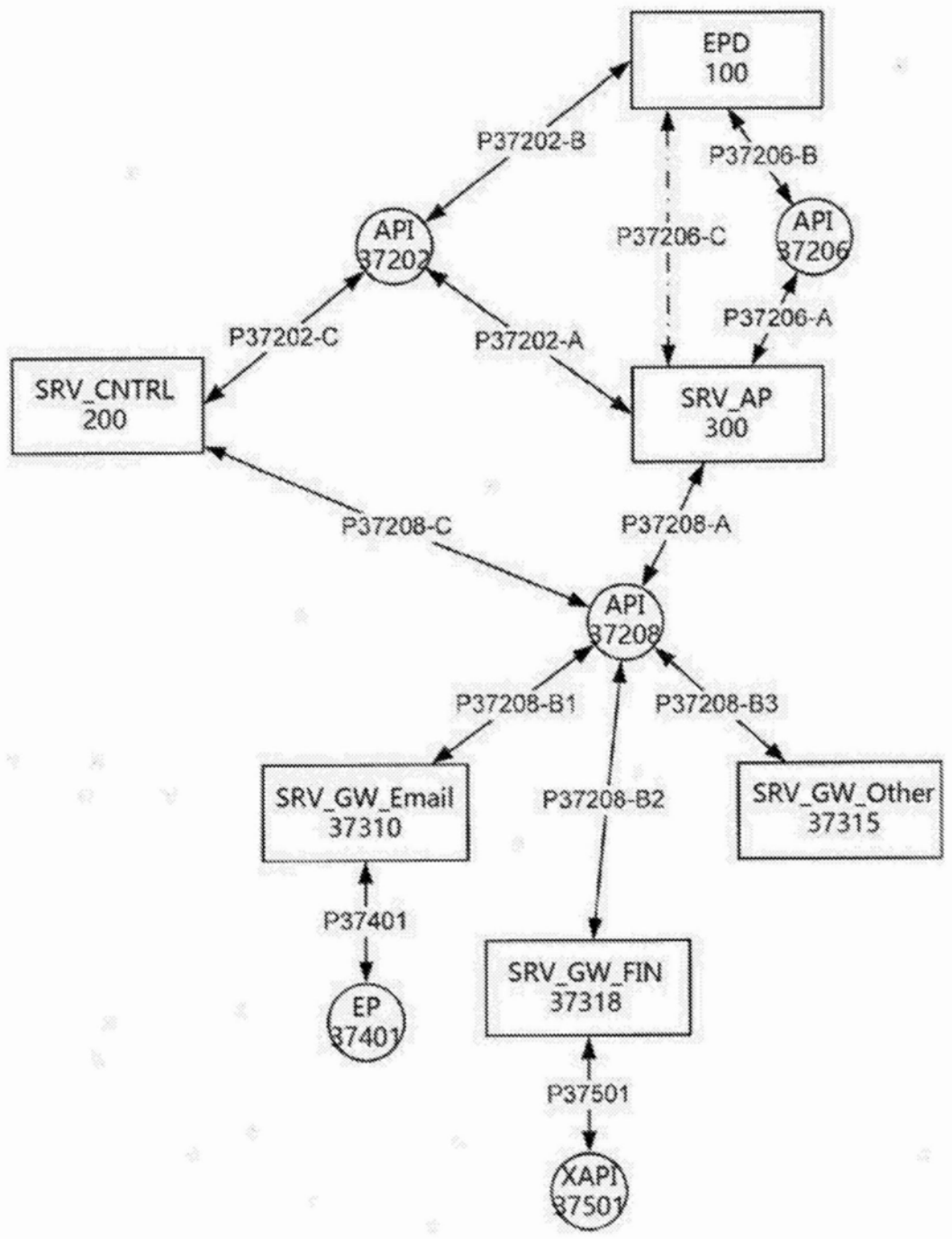

EPD
100
P37202-B
P37206-B
API
37202
P37206-C
API
37206
P37206-A
P37202-C
P37202-A
SRV_CNTRL
200
SRV_AP
300
P37208-C
P37208-A
API
37208
P37208-B1
P37208-B3
SRV_GW_Email
37310
P37208-B2
SRV_GW_Other
37315
P37401
EP
37401
SRV_GW_FIN
37318
P37501
XAPI
37501

图37

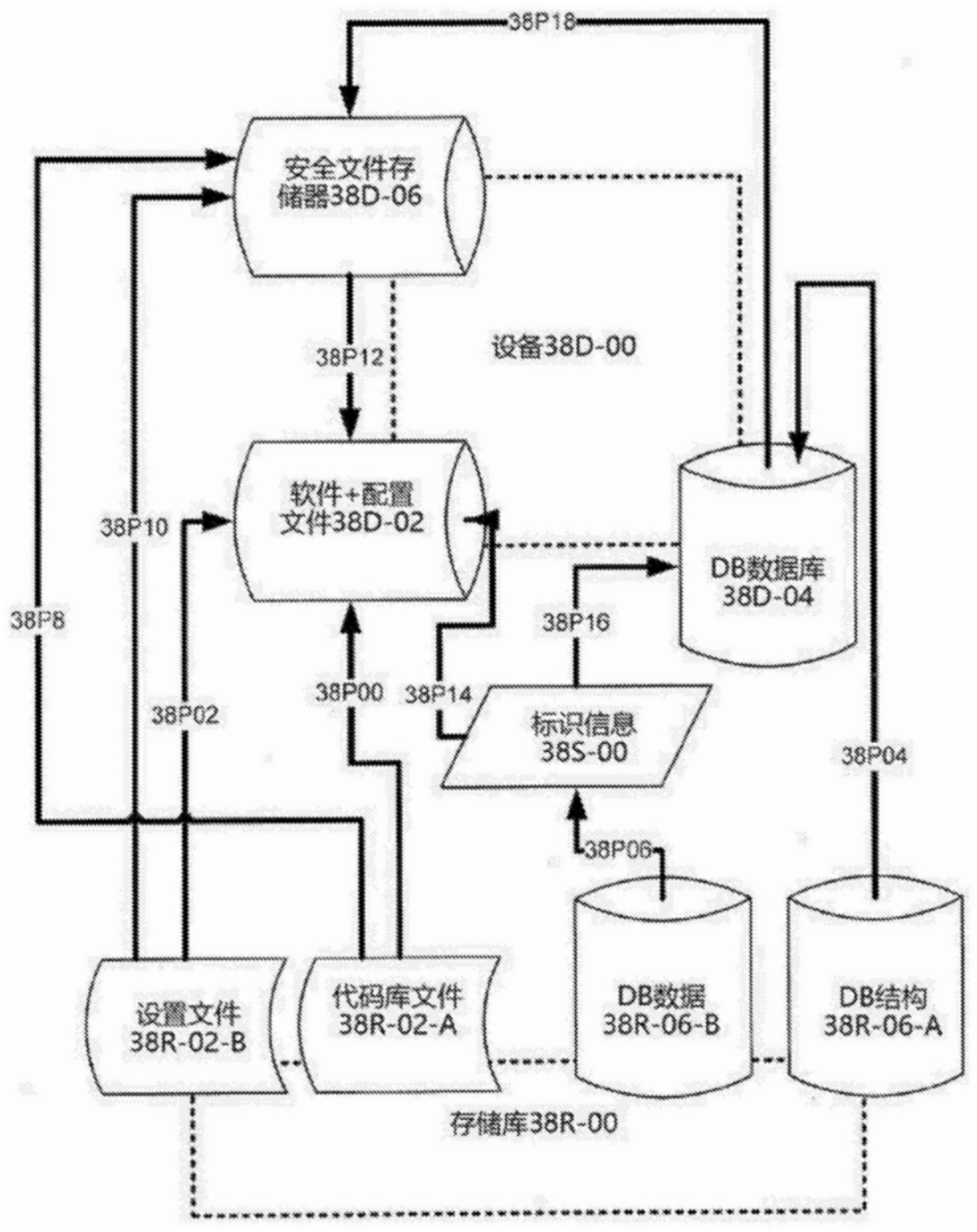

38P18
安全文件存储器38D-06
38P12
设备38D-00
软件+配置文件38D-02
38P10
38P8
DB数据库38D-04
38P16
38P00
38P14
38P02
标识信息38S-00
38P04
38P06
设置文件38R-02-B
代码库文件38R-02-A
DB数据38R-06-B
DB结构38R-06-A
存储库38R-00

图38

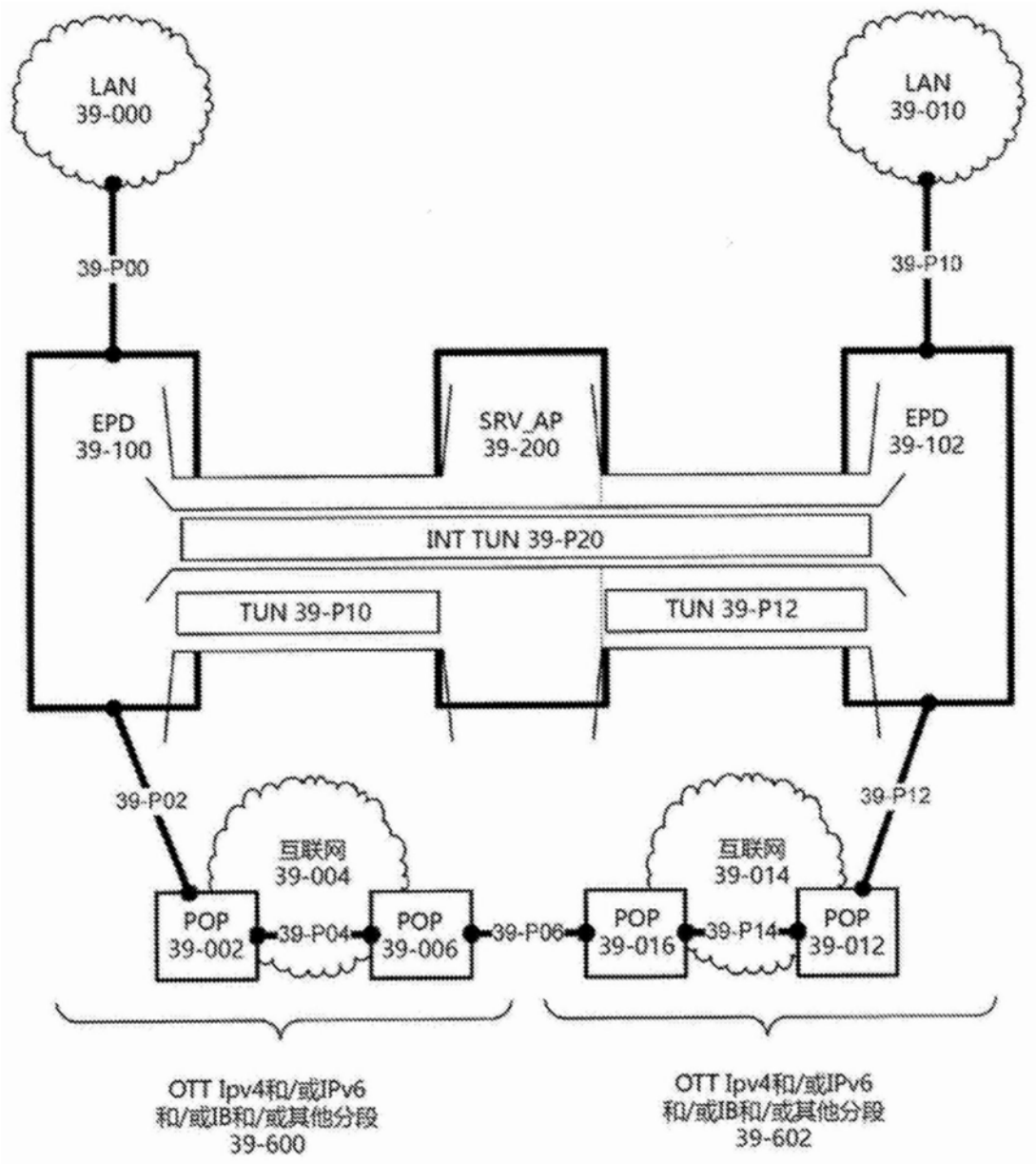

LAN
39-000
LAN
39-010
39-P00
39-P10
EPD
39-100
SRV_AP
39-200
EPD
39-102
INT TUN 39-P20
TUN 39-P10
TUN 39-P12
39-P02
39-P12
互联网
39-004
互联网
39-014
POP
39-002
39-P04
POP
39-006
39-P06
POP
39-016
39-P14
POP
39-012
OTT Ipv4和/或IPv6
和/或IB和/或其他分段
39-600
OTT Ipv4和/或IPv6
和/或IB和/或其他分段
39-602

图39

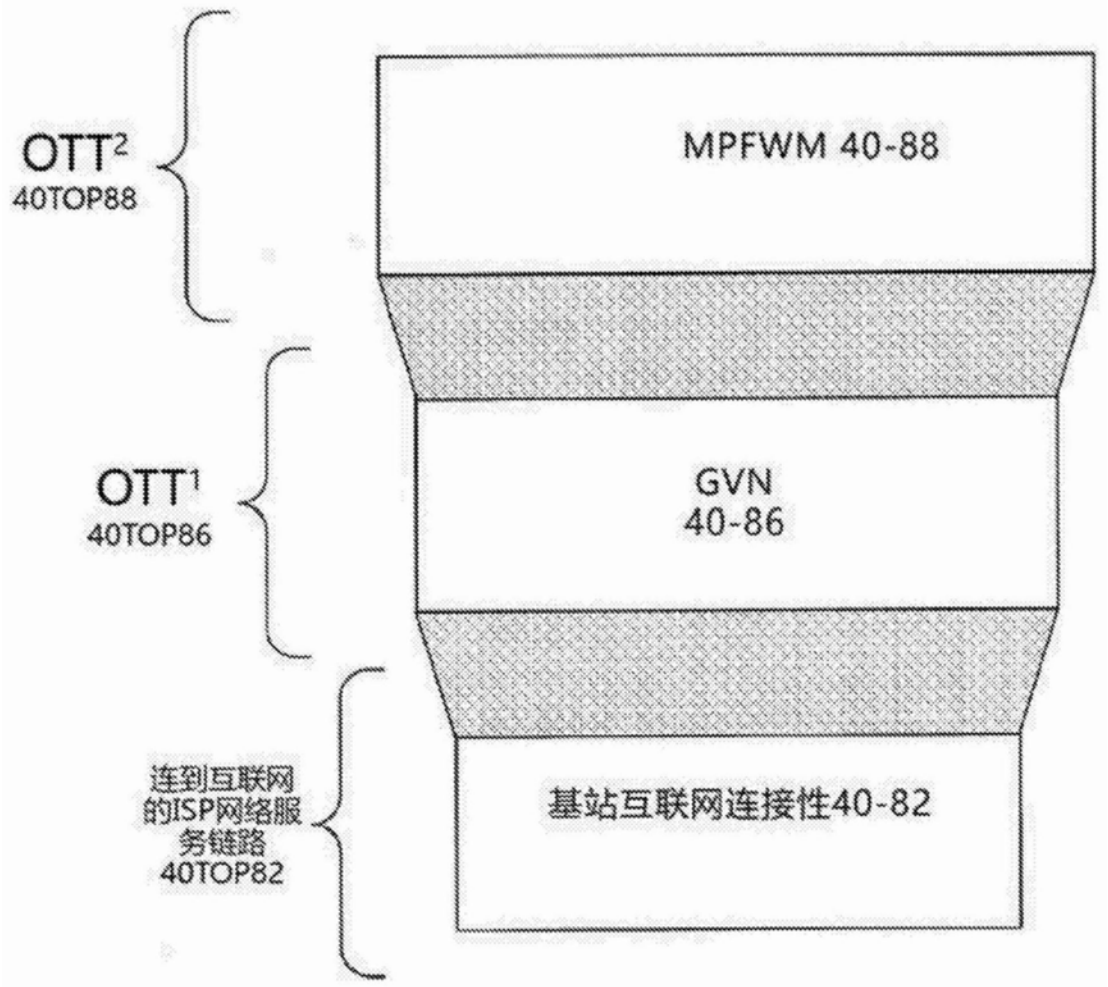

OTT2
40TOP88
MPFWM 40-88
OTT1
40TOP86
GVN
40-86
连到互联网
的ISP网络服
务链路
40TOP82
基站互联网连接性40-82

图40

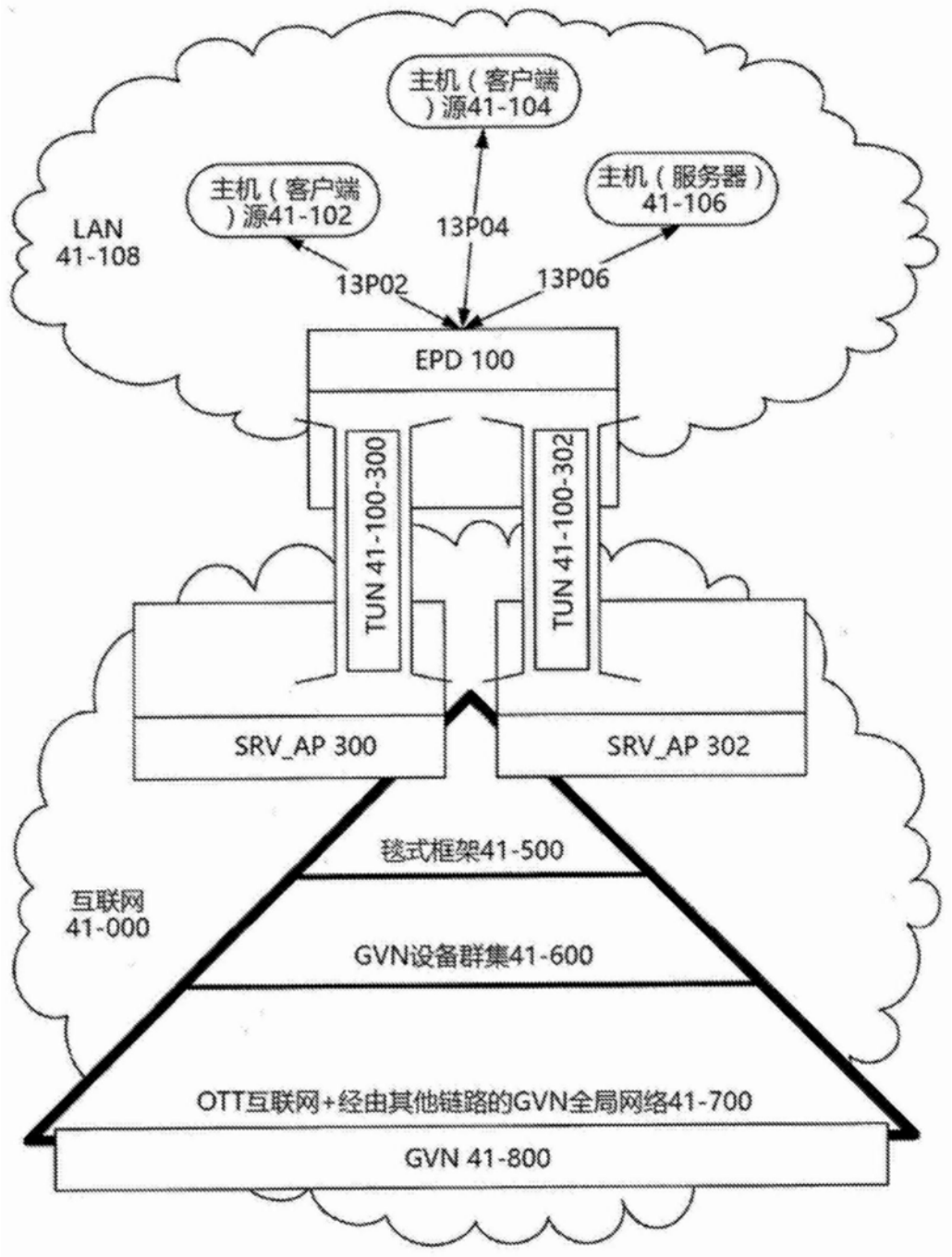

主机（客户端）源41-104
主机（客户端）源41-102
主机（服务器）41-106
LAN 41-108
13P04
13P02
13P06
EPD 100
TUN 41-100-300
TUN 41-100-302
SRV_AP 300
SRV_AP 302
毯式框架41-500
互联网 41-000
GVN设备群集41-600
OTT互联网+经由其他链路的GVN全局网络41-700
GVN 41-800

图41

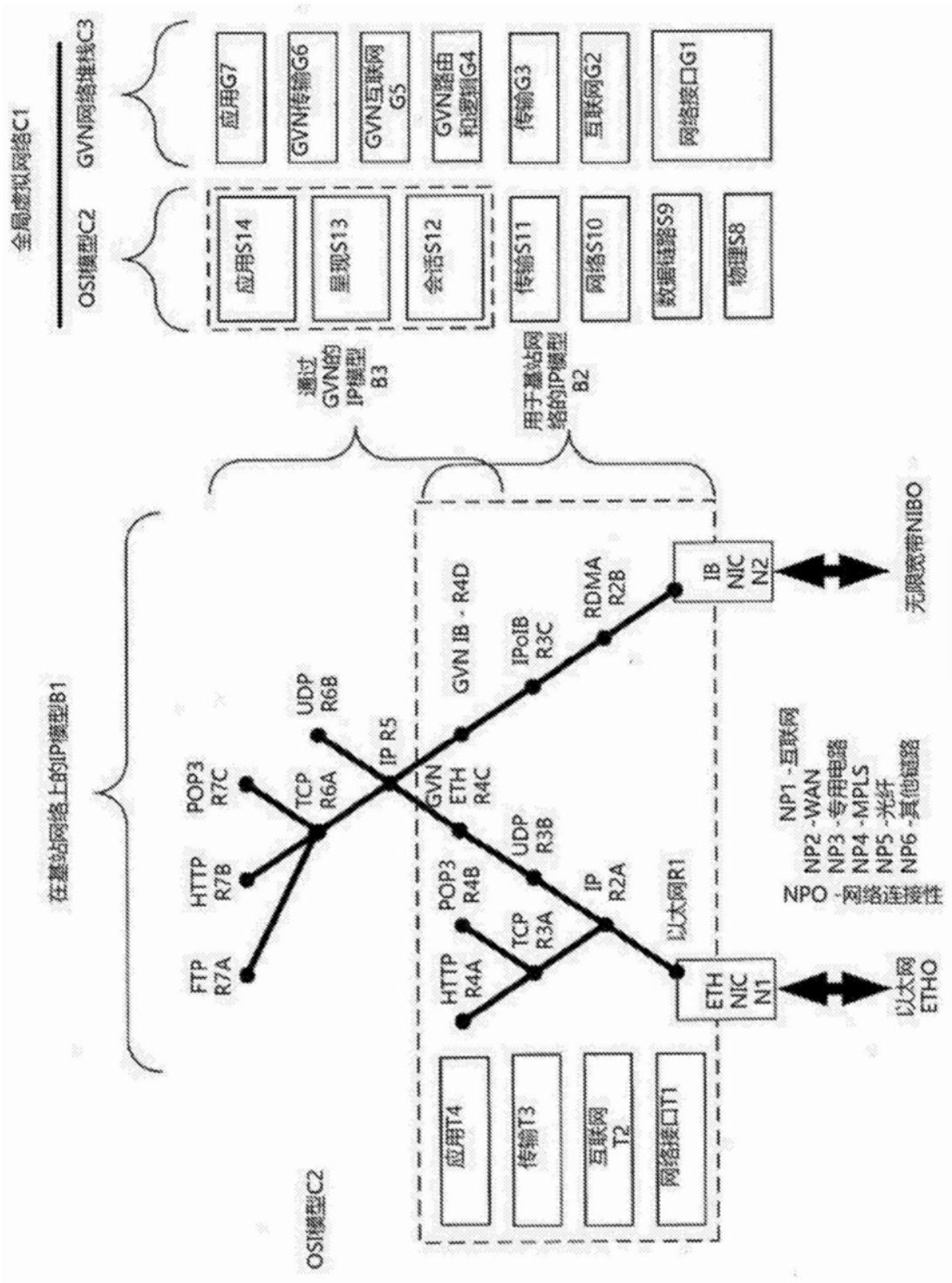

全局虚拟网络C1
GVN网络堆栈C3
OSI模型C2
应用G7
GVN传输G6
GVN互联网G5
GVN路由和逻辑G4
传输G3
互联网G2
网络接口G1
应用S14
呈现S13
会话S12
传输S11
网络S10
数据链路S9
物理S8
通过GVN的IP模型B3
用于基站网络的IP模型B2
在基站网络上的IP模型B1
UDP R6B
IP R5
GVN IB - R4D
IPoIB R3C
RDMA R2B
IB NIC N2
无限宽带NIBO
POP3 R7C
TCP R6A
GVN ETH R4C
HTTP R7B
UDP R3B
POP3 R4B
IP R2A
以太网R1
FTP R7A
TCP R3A
HTTP R4A
ETH NIC N1
以太网 ETHO
NP1 -互联网
NP2 -WAN
NP3 -专用电路
NP4 -MPLS
NP5 -光纤
NP6 -其他链路
NPO -网络连接性
应用T4
传输T3
互联网T2
网络接口T1
OSI模型C2

图42

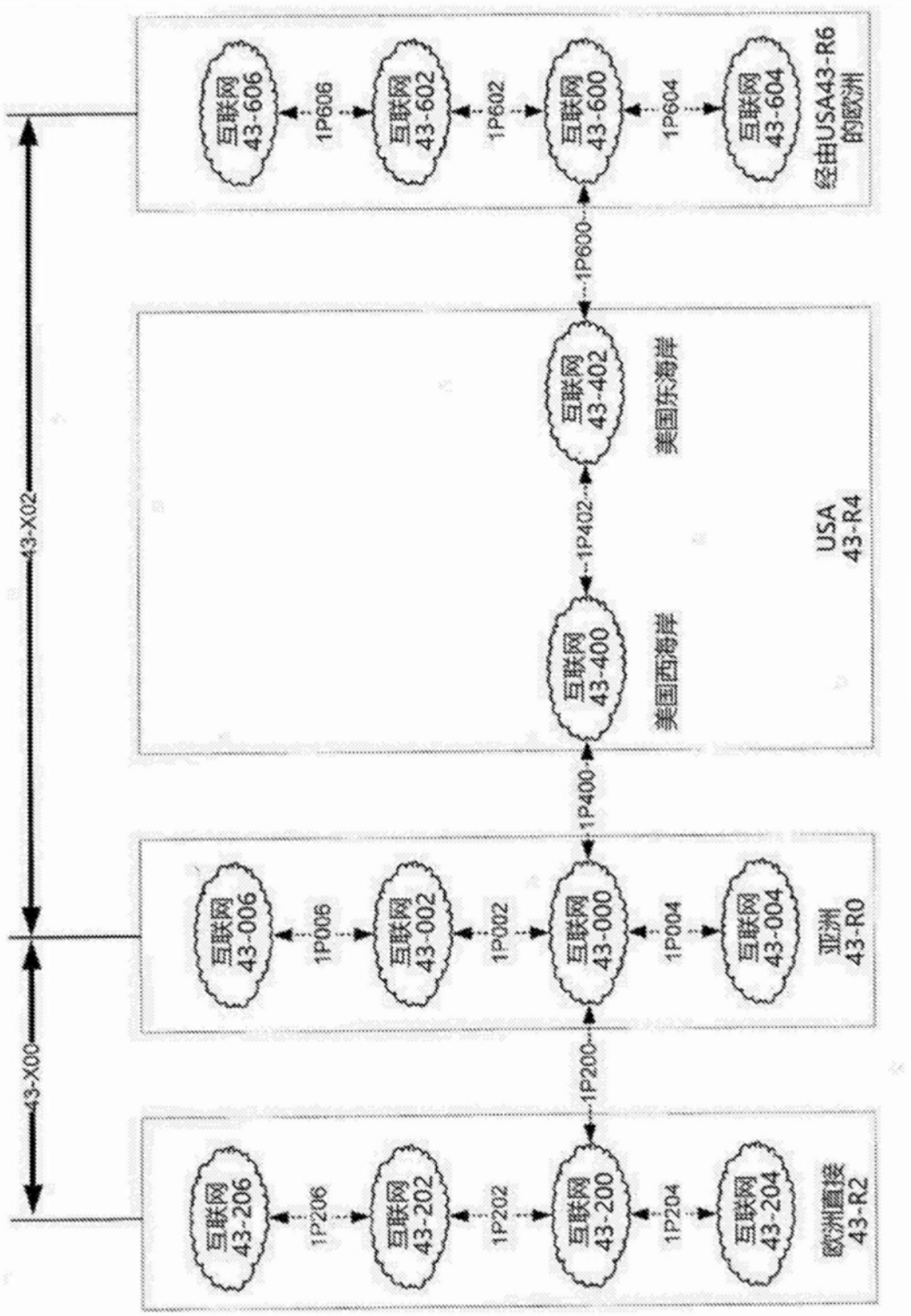

互联网 43-606
1P606
互联网 43-602
1P602
互联网 43-600
1P604
互联网 43-604
经由USA43-R6 的欧洲
1P600
互联网 43-402
美国东海岸
1P402
互联网 43-400
美国西海岸
USA 43-R4
1P400
互联网 43-006
1P006
互联网 43-002
1P002
互联网 43-000
1P004
互联网 43-004
亚洲 43-R0
1P200
互联网 43-206
1P206
互联网 43-202
1P202
互联网 43-200
1P204
互联网 43-204
欧洲直接 43-R2
43-X02
43-X00

图43

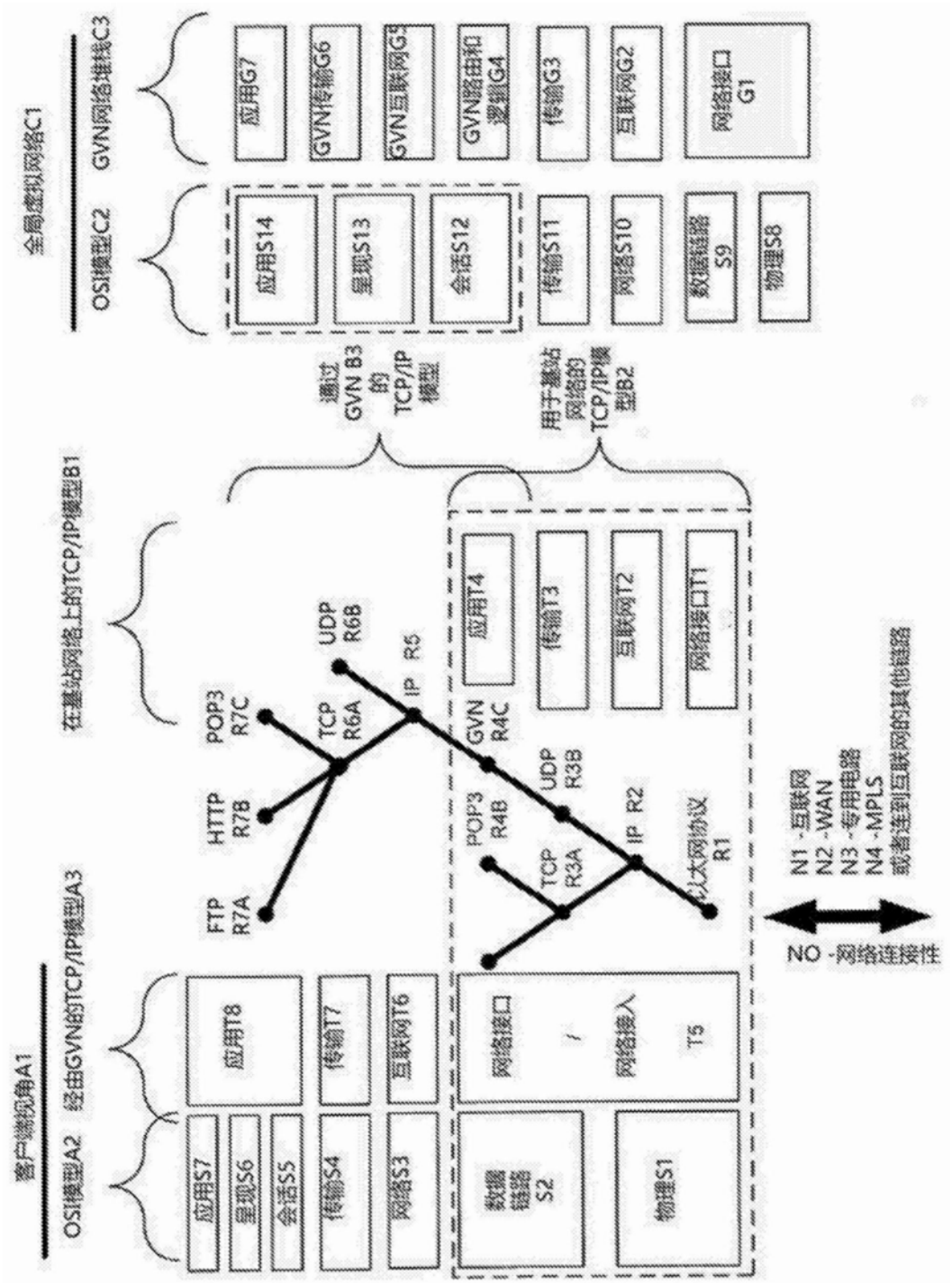

全局虚拟网络C1
GVN网络堆栈C3
OSI模型C2
应用G7
GVN传输G6
GVN互联网G5
GVN路由和逻辑G4
传输G3
互联网G2
网络接口G1
应用S14
呈现S13
会话S12
传输S11
网络S10
数据链路S9
物理S8
通过GVN B3的TCP/IP模型
用于基站网络的TCP/IP模型B2
在基站网络上的TCP/IP模型B1
客户端视角A1
经由GVN的TCP/IP模型A3
OSI模型A2
应用T8
传输T7
互联网T6
网络接口
网络接入
T5
应用S7
呈现S6
会话S5
传输S4
网络S3
数据链路S2
物理S1
应用T4
传输T3
互联网T2
网络接口T1
FTP R7A
HTTP R7B
POP3 R7C
TCP R6A
UDP R6B
IP R5
GVN R4C
POP3 R4B
TCP R3A
UDP R3B
IP R2
北大网协议 R1
N1 -互联网
N2 -WAN
N3 -专用电路
N4 -MPLS
或者连到互联网的其他链路
NO -网络连接性

图44

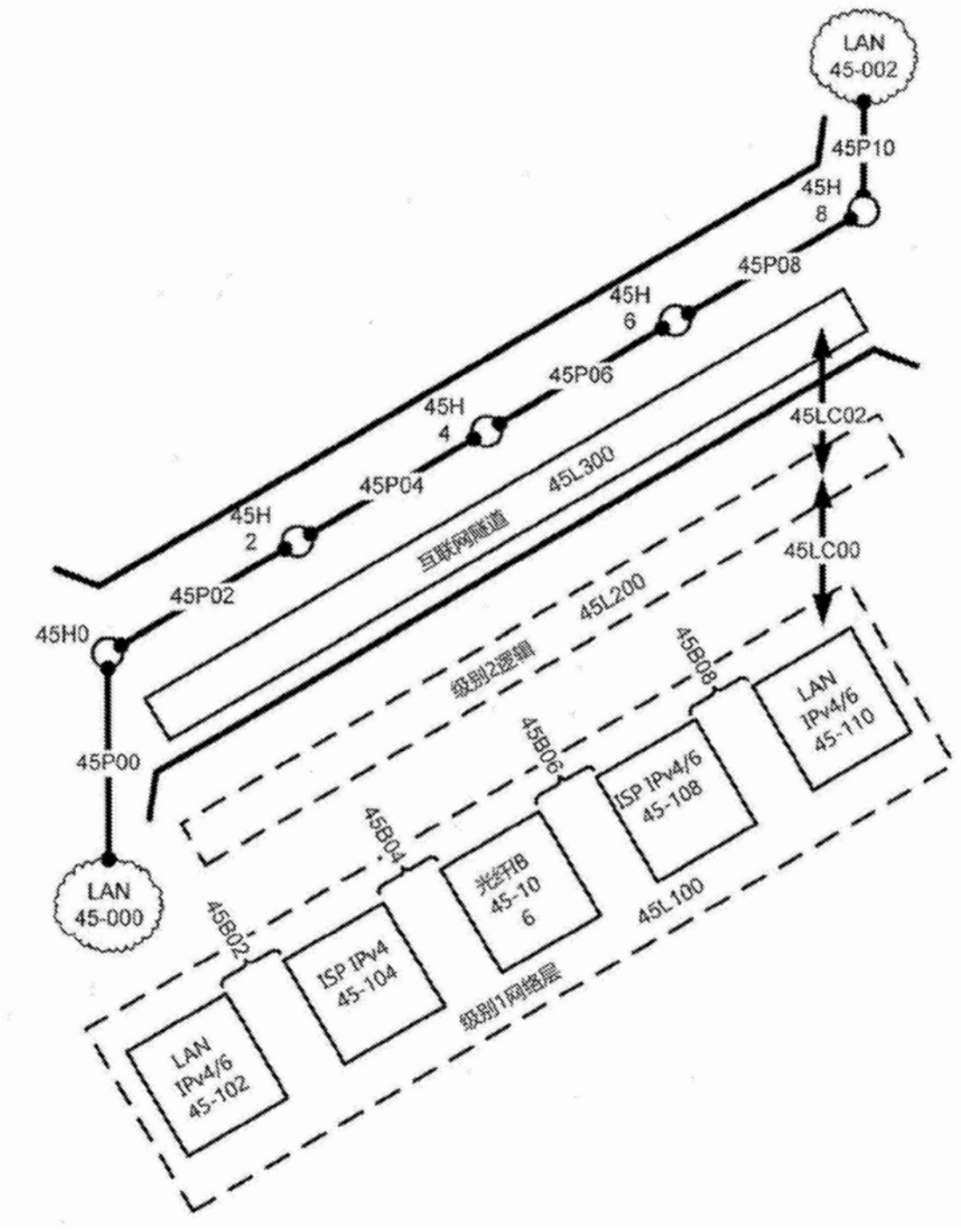

LAN
45-002
45P10
45H
8
45P08
45H
6
45P06
45H
4
45P04
45H
2
45P02
45H0
45P00
LAN
45-000
互联网隧道
45L300
45LC02
45LC00
45L200
级别2逻辑
45B08
45B06
45B04
45B02
LAN
IPv4/6
45-110
ISP IPv4/6
45-108
光纤IB
45-10
6
ISP IPv4
45-104
LAN
IPv4/6
45-102
45L100
级别1网络层

图45

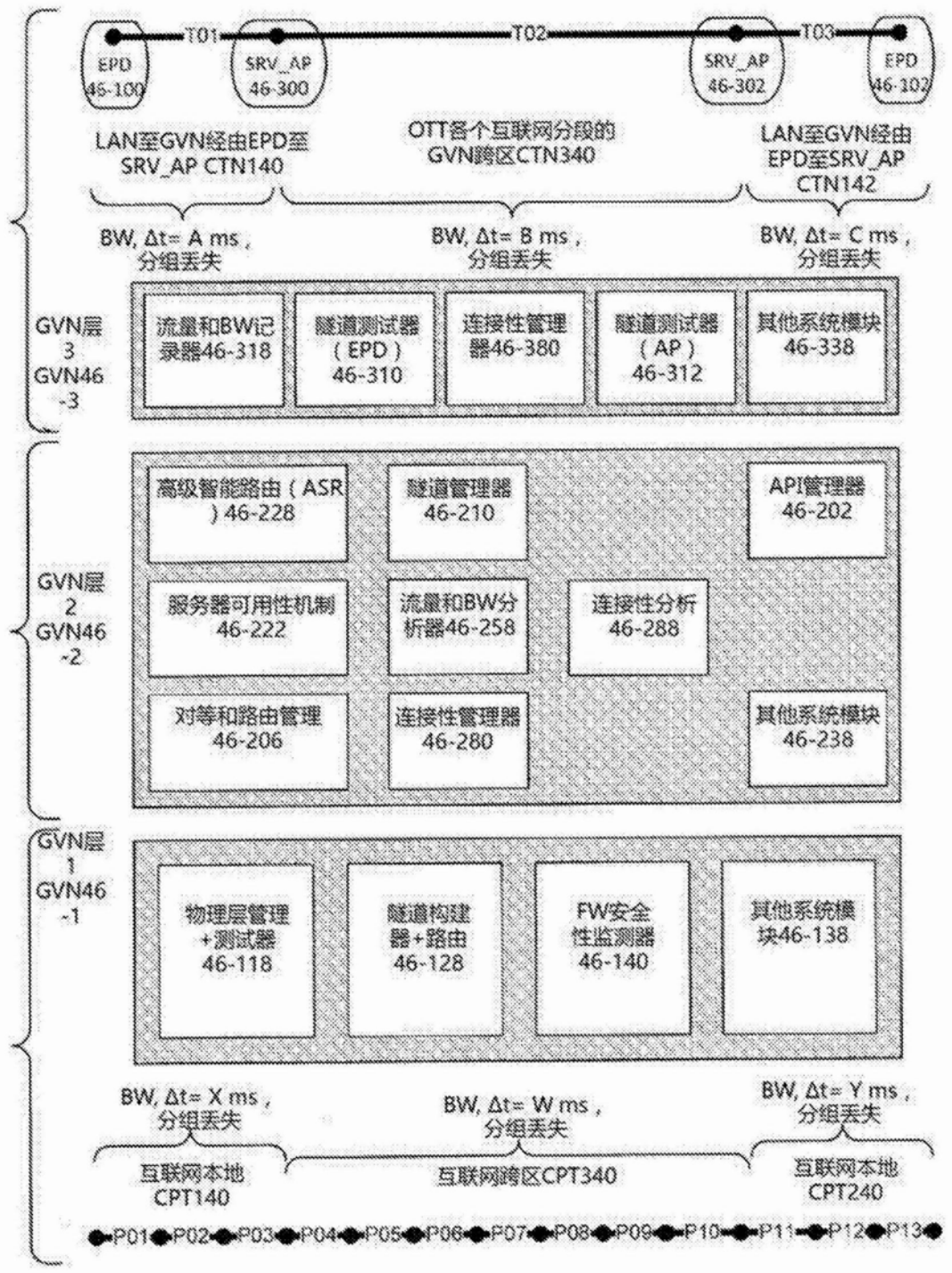

T01
T02
T03
EPD 46-100
SRV_AP 46-300
SRV_AP 46-302
EPD 46-102
LAN至GVN经由EPD至SRV_AP CTN140
OTT各个互联网分段的GVN跨区CTN340
LAN至GVN经由EPD至SRV_AP CTN142
BW, Δt= A ms, 分组丢失
BW, Δt= B ms, 分组丢失
BW, Δt= C ms, 分组丢失
GVN层3 GVN46-3
流量和BW记录器46-318
隧道测试器（EPD）46-310
连接性管理器46-380
隧道测试器（AP）46-312
其他系统模块46-338
GVN层2 GVN46-2
高级智能路由（ASR）46-228
隧道管理器46-210
API管理器46-202
服务器可用性机制46-222
流量和BW分析器46-258
连接性分析46-288
对等和路由管理46-206
连接性管理器46-280
其他系统模块46-238
GVN层1 GVN46-1
物理层管理+测试器46-118
隧道构建器+路由46-128
FW安全性监测器46-140
其他系统模块46-138
BW, Δt= X ms, 分组丢失
BW, Δt= W ms, 分组丢失
BW, Δt= Y ms, 分组丢失
互联网本地CPT140
互联网跨区CPT340
互联网本地CPT240
P01 P02 P03 P04 P05 P06 P07 P08 P09 P10 P11 P12 P13

图46

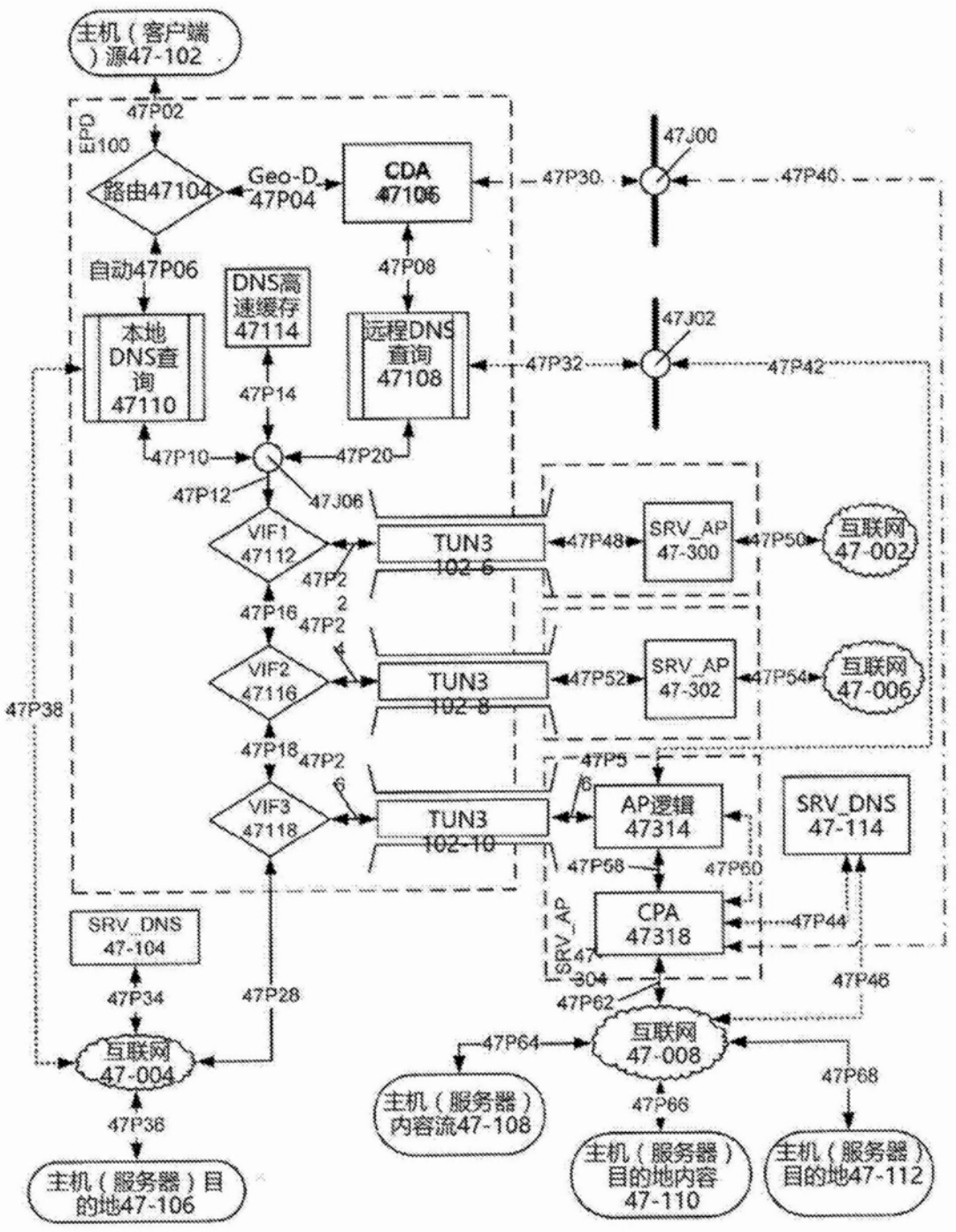

主机（客户端）源47-102
47P02
47100
路由47104
Geo-D 47P04
CDA 47106
47P30
47J00
47P40
自动47P06
DNS高速缓存 47114
47P08
本地DNS查询 47110
远程DNS查询 47108
47J02
47P32
47P42
47P14
47P10
47P20
47P12
47J06
VIF1 47112
TUN3 102-6
47P48
SRV_AP 47-300
47P50
互联网 47-002
47P22
47P16
47P24
VIF2 47116
TUN3 102-8
47P52
SRV_AP 47-302
47P54
互联网 47-006
47P38
47P18
47P26
47P56
VIF3 47118
TUN3 102-10
AP逻辑 47314
SRV_DNS 47-114
47P58
47P60
CPA 47318
47P44
SRV_AP 47-304
SRV_DNS 47-104
47P34
47P28
47P62
47P46
互联网 47-004
47P64
互联网 47-008
47P68
47P66
主机（服务器）内容流47-108
主机（服务器）目的地内容 47-110
主机（服务器）目的地47-112
47P36
主机（服务器）目的地47-106

图47

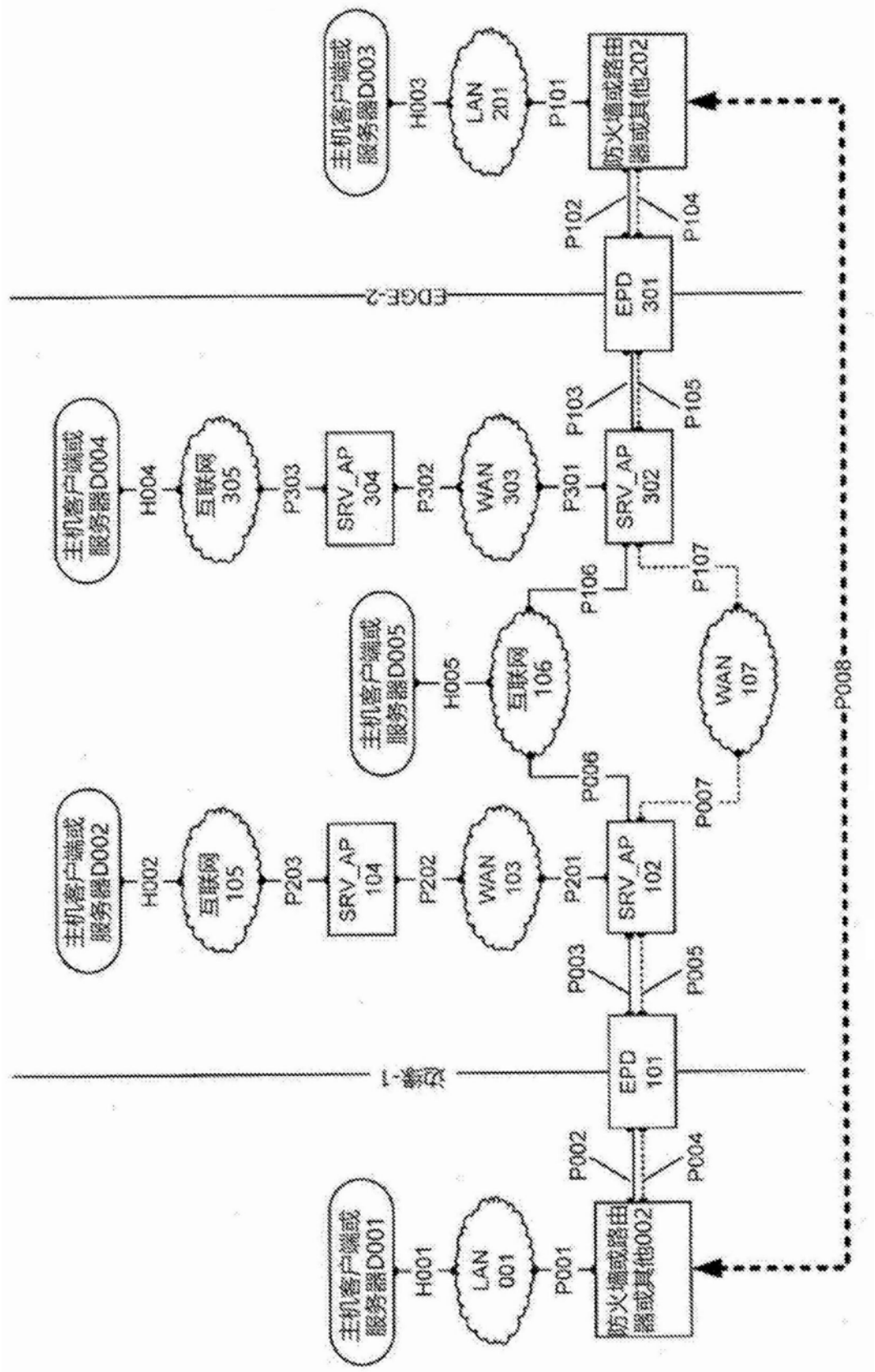

主机客户端或服务器D001
H001
LAN 001
P001
防火墙或路由器或其他002
P002
P004
EPD 101
P003
P005
SRV_AP 102
P201
WAN 103
P202
SRV_AP 104
P203
互联网 105
H002
主机客户端或服务器D002
P006
P007
互联网 106
H005
主机客户端或服务器D005
WAN 107
P008
P106
P107
SRV_AP 302
P301
WAN 303
P302
SRV_AP 304
P303
互联网 305
H004
主机客户端或服务器D004
P103
P105
EPD 301
P102
P104
防火墙或路由器或其他202
P101
LAN 201
H003
主机客户端或服务器D003

图48

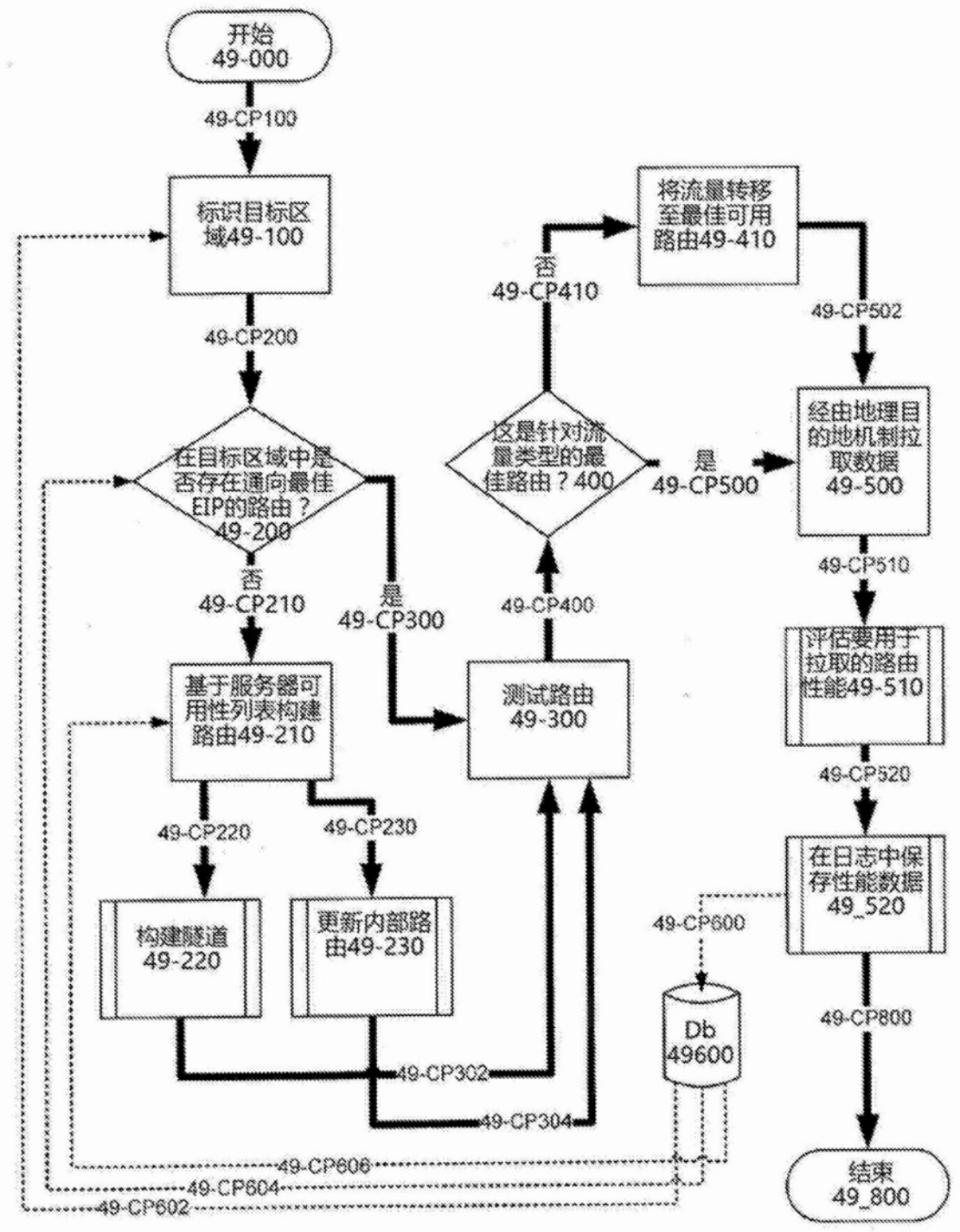

开始
49-000
49-CP100
标识目标区域49-100
49-CP200
在目标区域中是否存在通向最佳EIP的路由？
49-200
否
49-CP210
是
49-CP300
基于服务器可用性列表构建路由49-210
49-CP220
49-CP230
构建隧道
49-220
更新内部路由49-230
测试路由
49-300
49-CP400
这是针对流量类型的最佳路由？400
否
49-CP410
将流量转移至最佳可用路由49-410
是
49-CP500
49-CP502
经由地理目的地机制拉取数据
49-500
49-CP510
评估要用于拉取的路由性能49-510
49-CP520
在日志中保存性能数据
49_520
49-CP600
Db
49600
49-CP800
结束
49_800
49-CP302
49-CP304
49-CP606
49-CP604
49-CP602

图49

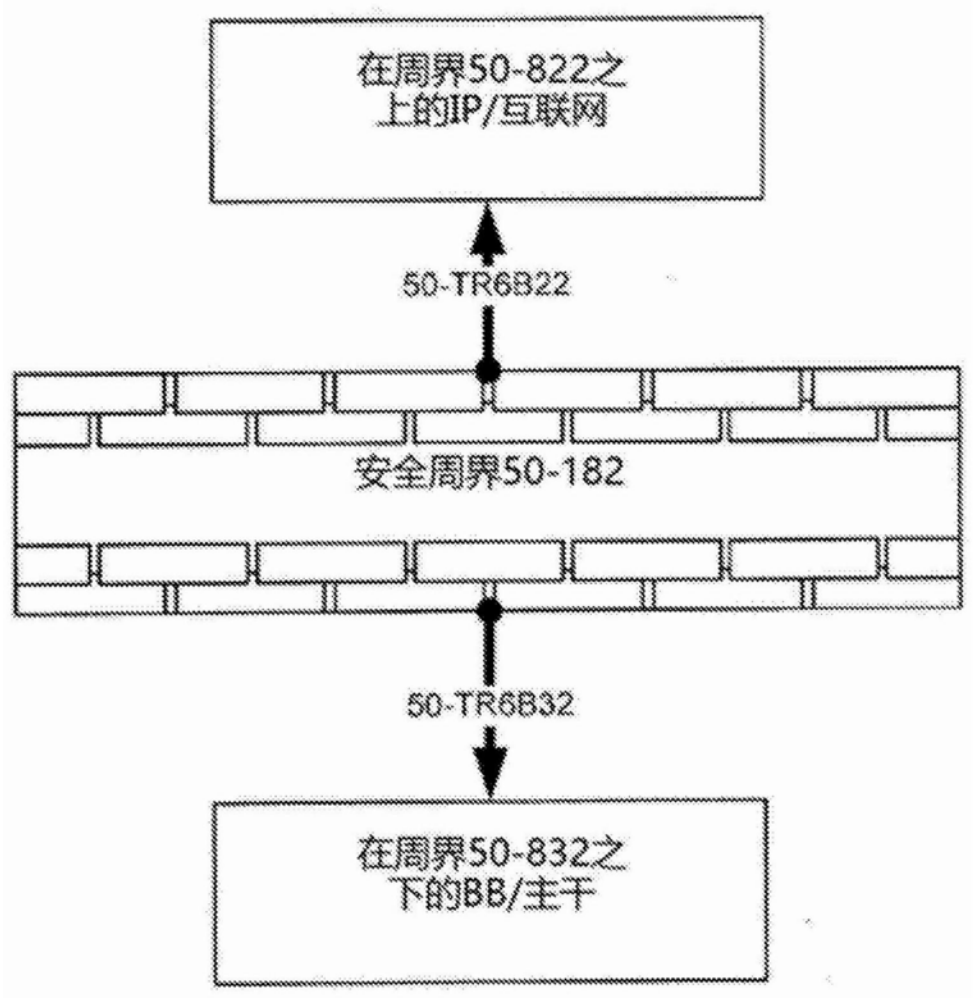

在周界50-822之
上的IP/互联网
50-TR6B22
安全周界50-182
50-TR6B32
在周界50-832之
下的BB/主干

图50

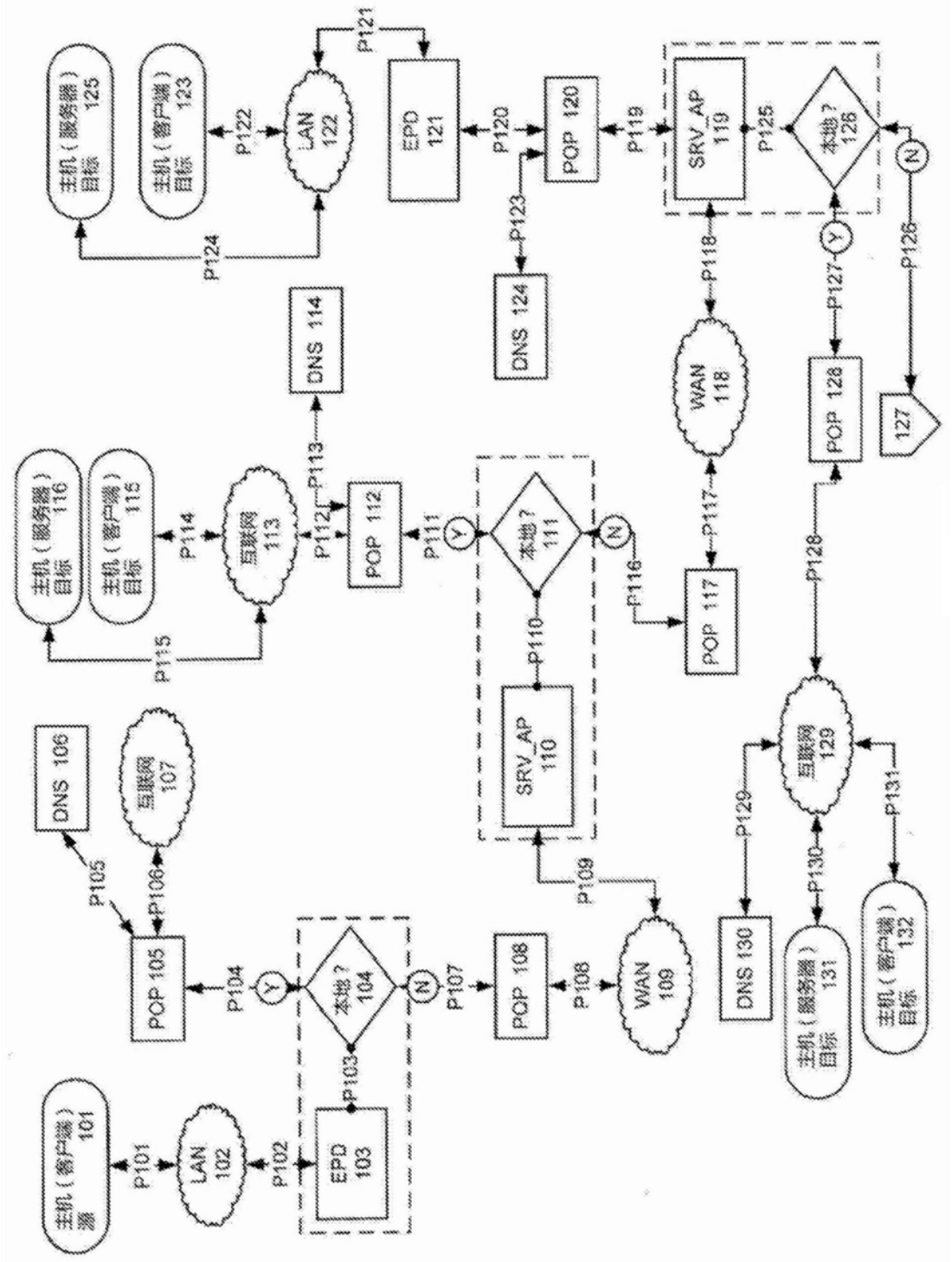

主机（客户端）
101
LAN
102
EPD
103
本地？
104
POP 105
DNS 106
互联网
107
POP 108
WAN
109
SRV_AP
110
本地？
111
POP 112
DNS 114
互联网
113
主机（客户端）
115
主机（服务器）
116
P101
P102
P103
P104
P105
P106
P107
P108
P109
P110
P111
P112
P113
P114
P115
P116
POP 117
WAN
118
SRV_AP
119
POP 120
EPD
121
LAN
122
主机（客户端）
123
主机（服务器）
125
DNS 124
本地？
126
POP 128
127
互联网
129
DNS 130
主机（服务器）
131
主机（客户端）
132
P117
P118
P120
P121
P122
P123
P124
P125
P126
P127
P128
P129
P130
P131
Y
N

图51

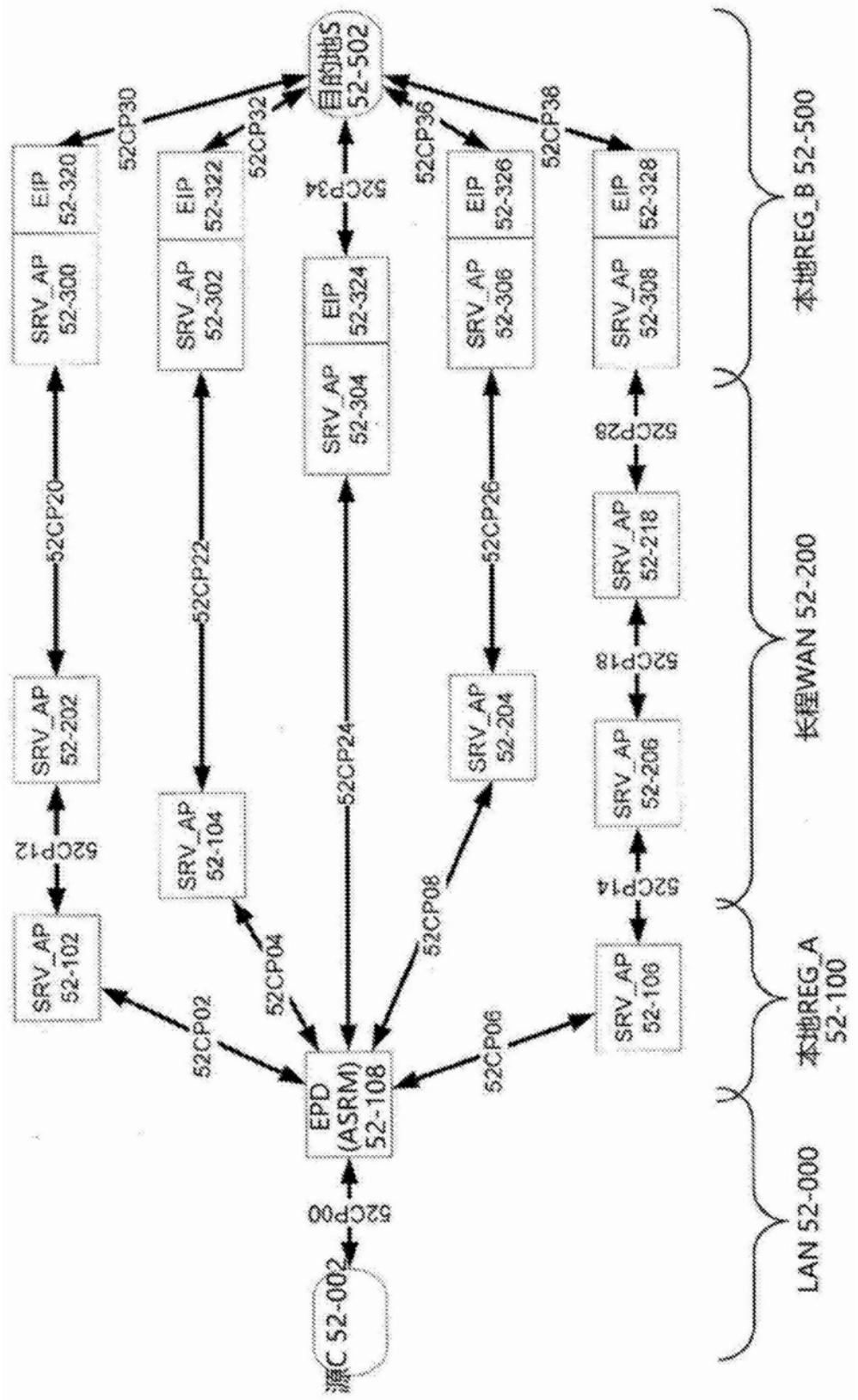

目的地S 52-502
52CP30
52CP32
52CP34
52CP36
52CP38
EIP 52-320
SRV_AP 52-300
EIP 52-322
SRV_AP 52-302
EIP 52-324
SRV_AP 52-304
EIP 52-326
SRV_AP 52-306
EIP 52-328
SRV_AP 52-308
本地REG_B 52-500
52CP20
52CP22
52CP24
52CP26
52CP28
SRV_AP 52-218
52CP18
SRV_AP 52-202
SRV_AP 52-104
SRV_AP 52-204
SRV_AP 52-206
52CP12
52CP08
52CP14
长程WAN 52-200
SRV_AP 52-102
52CP02
52CP04
52CP06
SRV_AP 52-106
EPD (ASRM) 52-108
本地REG_A 52-100
52CP00
源C 52-002
LAN 52-000

图52

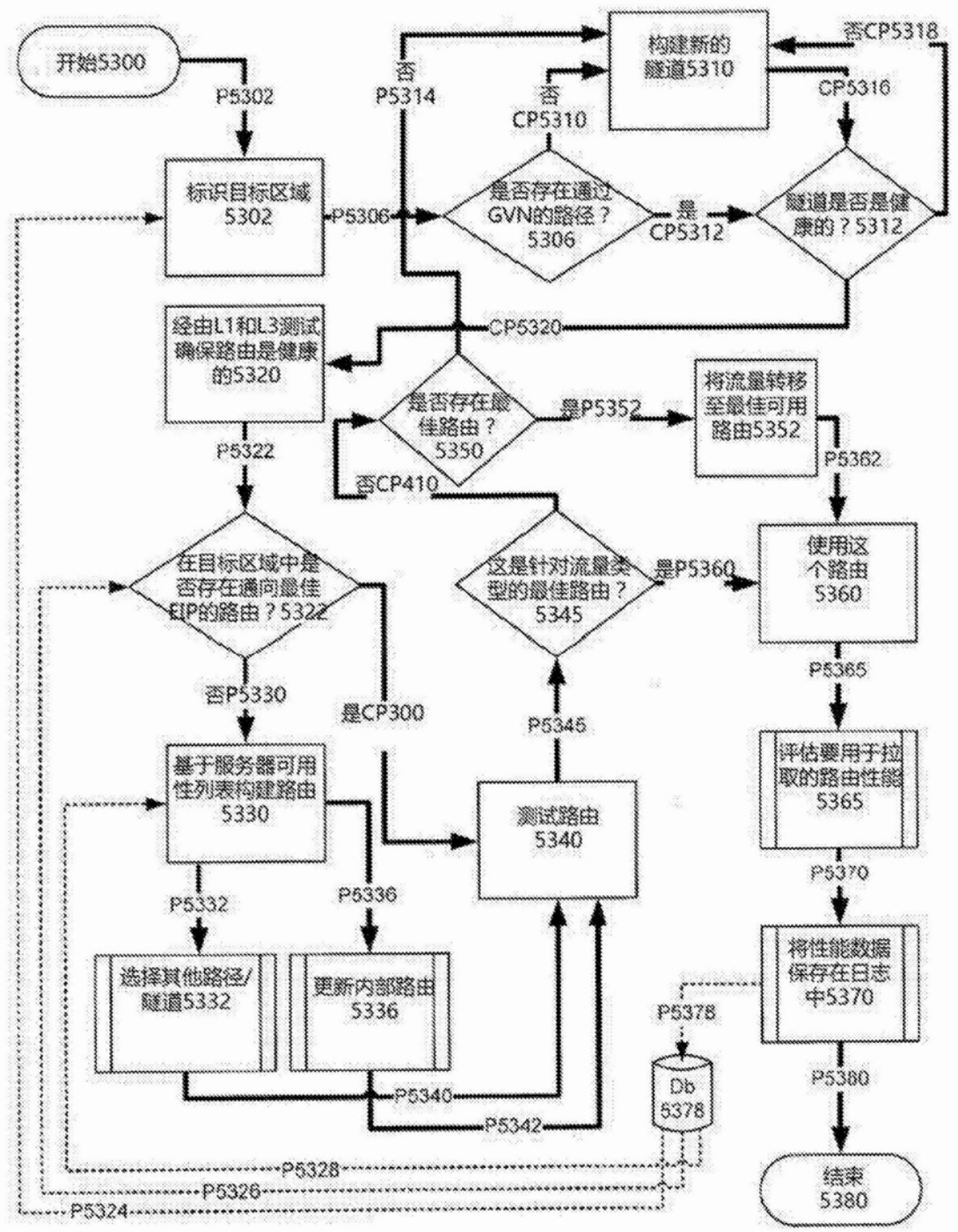

开始5300
P5302
标识目标区域5302
P5306
是否存在通过GVN的路径？5306
否P5314
否CP5310
构建新的隧道5310
否CP5318
CP5316
是CP5312
隧道是否是健康的？5312
经由L1和L3测试确保路由是健康的5320
CP5320
P5322
是否存在最佳路由？5350
是P5352
将流量转移至最佳可用路由5352
P5362
否CP410
在目标区域中是否存在通向最佳EIP的路由？5322
这是针对流量类型的最佳路由？5345
是P5360
使用这个路由5360
P5365
否P5330
是CP300
P5345
基于服务器可用性列表构建路由5330
测试路由5340
评估要用于拉取的路由性能5365
P5370
P5332
P5336
选择其他路径/隧道5332
更新内部路由5336
将性能数据保存在日志中5370
P5378
Db 5378
P5380
P5340
P5342
结束5380
P5328
P5326
P5324

图53

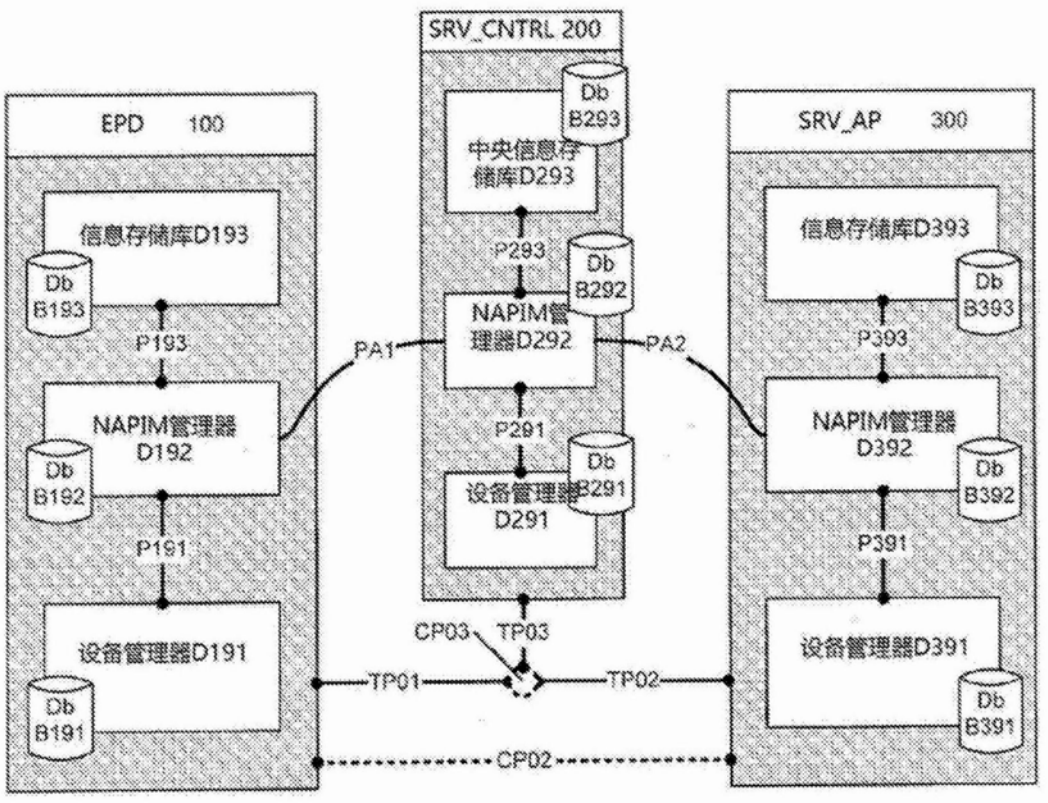

SRV_CNTRL 200
Db B293
中央信息存储库D293
P293
Db B292
NAPIM管理器D292
P291
Db B291
设备管理器D291
EPD 100
信息存储库D193
Db B193
P193
NAPIM管理器D192
Db B192
P191
设备管理器D191
Db B191
SRV_AP 300
信息存储库D393
Db B393
P393
NAPIM管理器D392
Db B392
P391
设备管理器D391
Db B391
PA1
PA2
CP03
TP03
TP01
TP02
CP02

图54

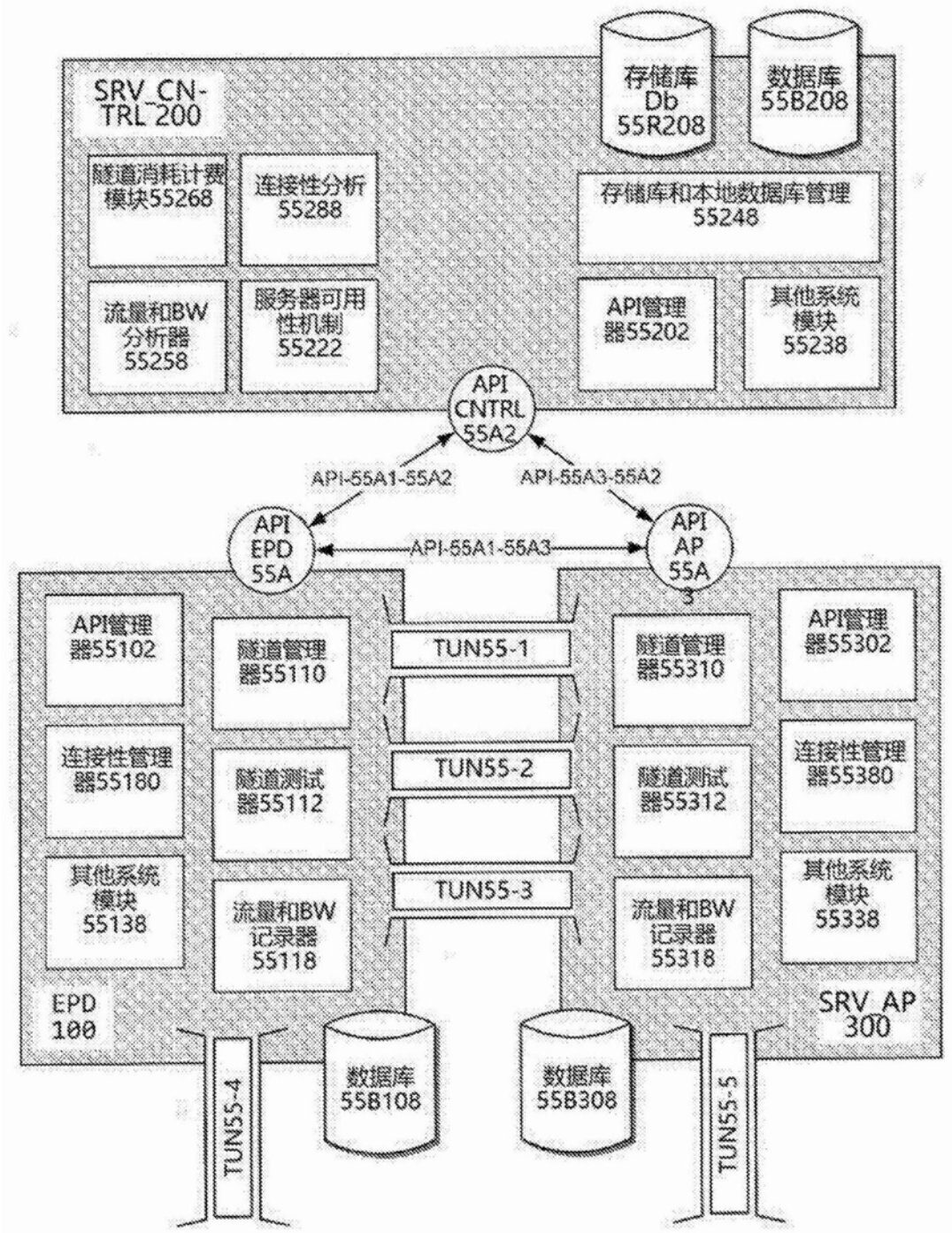

SRV_CN-TRL 200
存储库 Db 55R208
数据库 55B208
隧道消耗计费模块55268
连接性分析 55288
存储库和本地数据库管理 55248
流量和BW分析器 55258
服务器可用性机制 55222
API管理器55202
其他系统模块 55238
API CNTRL 55A2
API-55A1-55A2
API-55A3-55A2
API EPD 55A
API-55A1-55A3
API AP 55A 3
API管理器55102
隧道管理器55110
TUN55-1
隧道管理器55310
API管理器55302
连接性管理器55180
隧道测试器55112
TUN55-2
隧道测试器55312
连接性管理器55380
其他系统模块 55138
流量和BW记录器 55118
TUN55-3
流量和BW记录器 55318
其他系统模块 55338
EPD 100
SRV_AP 300
TUN55-4
数据库 55B108
数据库 55B308
TUN55-5

图55

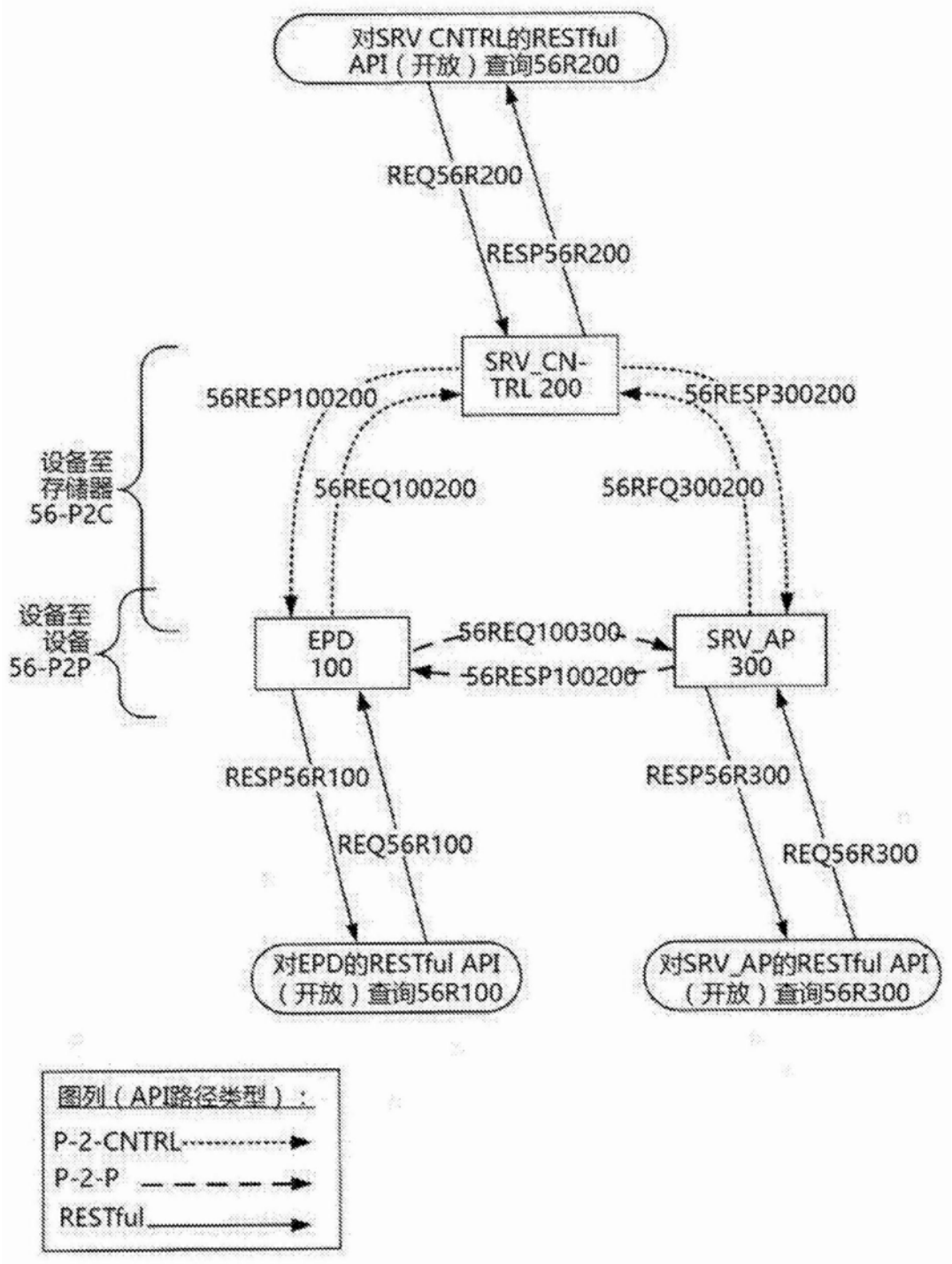

对SRV CNTRL的RESTful API（开放）查询56R200
REQ56R200
RESP56R200
SRV_CN-TRL 200
56RESP100200
56RESP300200
56REQ100200
56RFQ300200
设备至存储器56-P2C
设备至设备56-P2P
EPD 100
SRV_AP 300
56REQ100300
56RESP100200
RESP56R100
REQ56R100
RESP56R300
REQ56R300
对EPD的RESTful API（开放）查询56R100
对SRV_AP的RESTful API（开放）查询56R300
图列（API路径类型）：
P-2-CNTRL
P-2-P
RESTful

图56

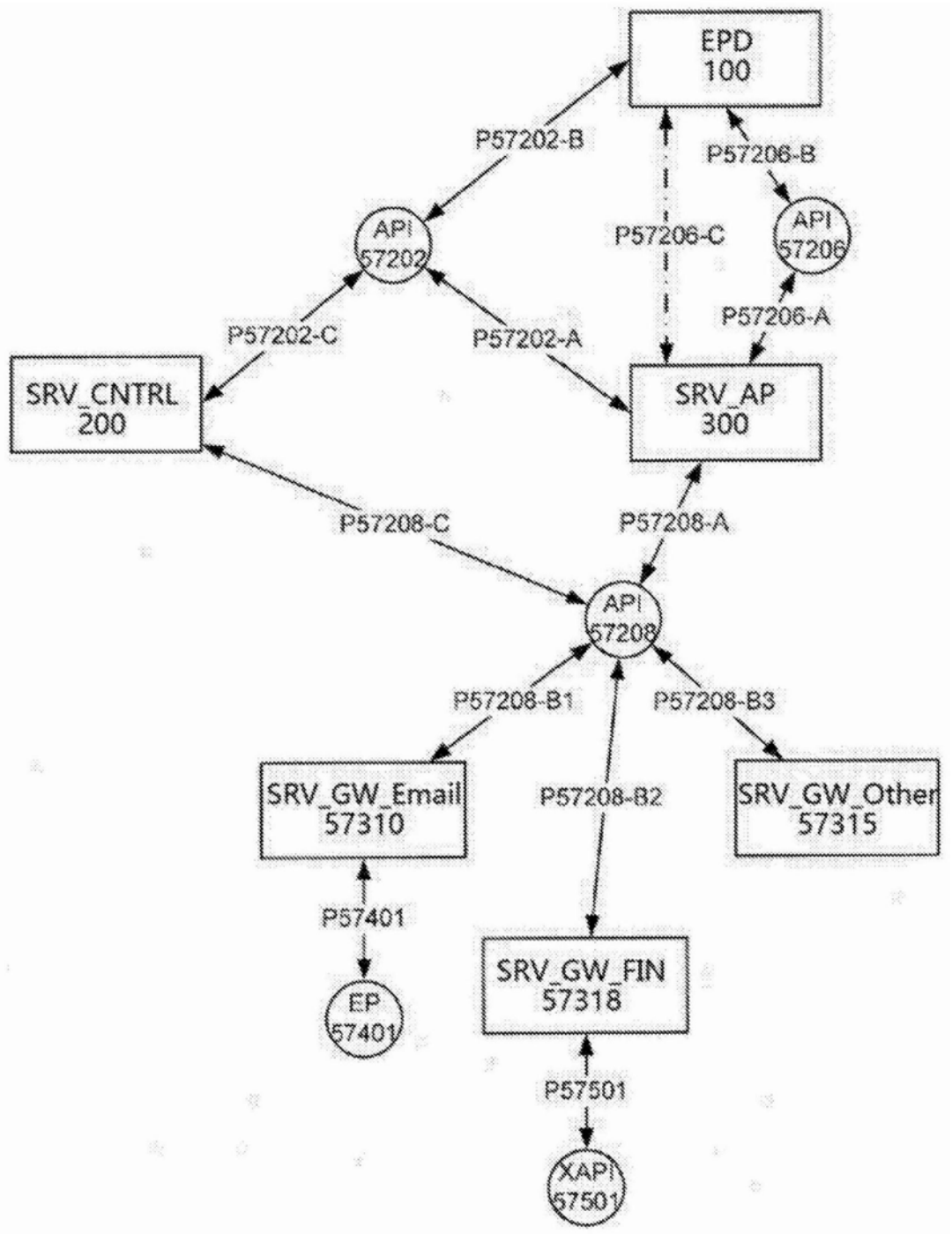

EPD
100
P57202-B
P57206-B
API
57202
P57206-C
API
57206
P57202-C
P57202-A
P57206-A
SRV_CNTRL
200
SRV_AP
300
P57208-C
P57208-A
API
57208
P57208-B1
P57208-B3
SRV_GW_Email
57310
P57208-B2
SRV_GW_Other
57315
P57401
EP
57401
SRV_GW_FIN
57318
P57501
XAPI
57501

图57

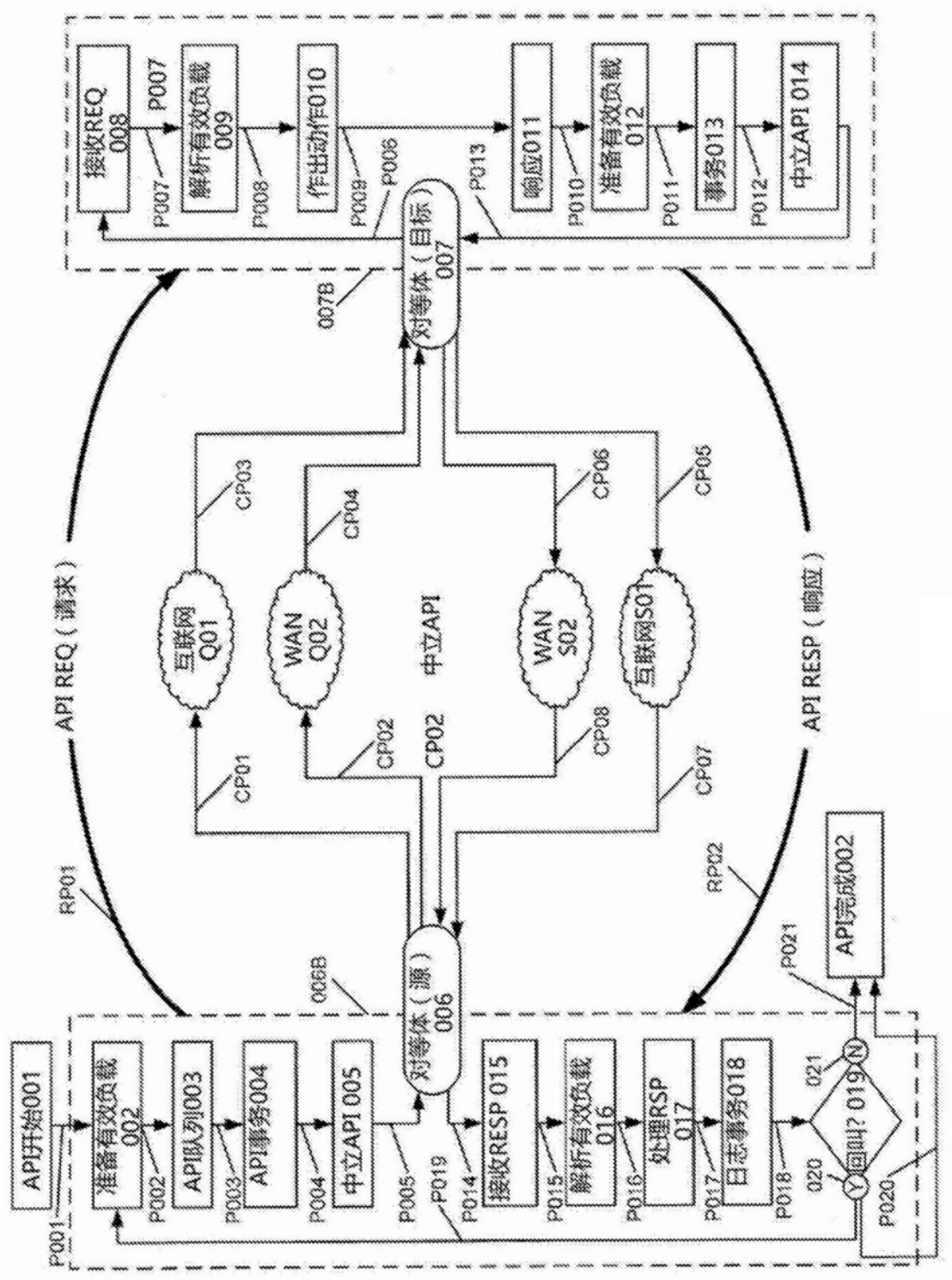

API开始001
准备有效负载002
API队列003
API事务004
中立API 005
对等体（源）006
接收RESP 015
解析有效负载016
处理RSP 017
日志事务018
回叫? 019
API完成002
接收REQ 008
解析有效负载009
作出动作010
响应011
准备有效负载012
事务013
中立API 014
对等体（目标）007
互联网Q01
WAN Q02
中立API
WAN S02
互联网S01
API REQ（请求）
API RESP（响应）

图58

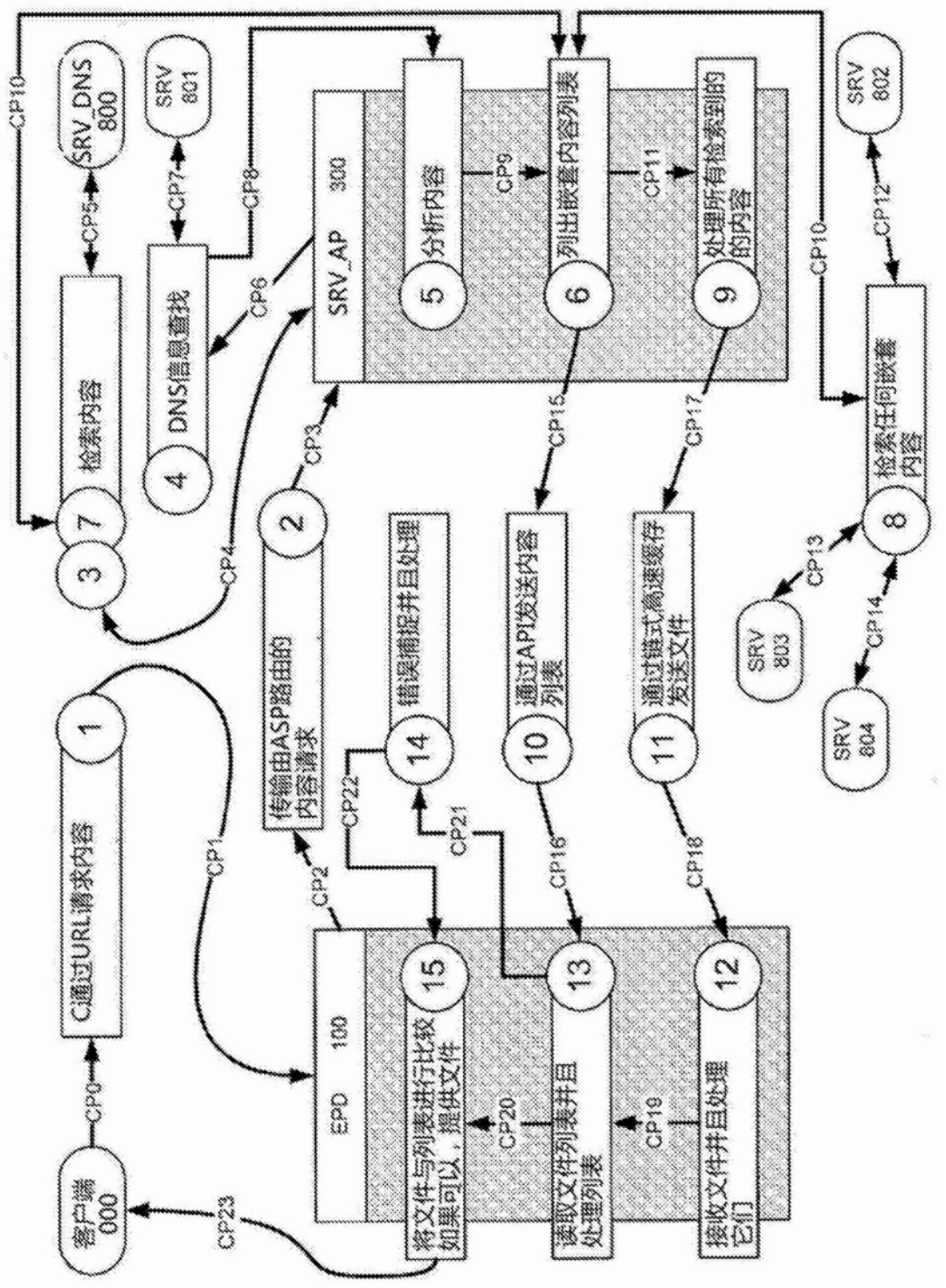

客户端 000
SRV_DNS 800
SRV 801
SRV 802
SRV 803
SRV 804
EPD 100
SRV_AP 300
C通过URL请求内容
检索内容
DNS信息查找
传输由ASP路由的内容请求
分析内容
列出嵌套内容列表
处理所有检索到的的内容
检索任何嵌套内容
错误捕捉并且处理
通过API发送内容列表
通过链式编译缓存发送文件
将文件与列表进行比较如果可以，提供文件
读取文件列表并且处理列表
接收文件并且处理它们
CP1
CP2
CP3
CP4
CP5
CP6
CP7
CP8
CP9
CP10
CP11
CP12
CP13
CP14
CP15
CP16
CP17
CP18
CP19
CP20
CP21
CP22
CP23

图59

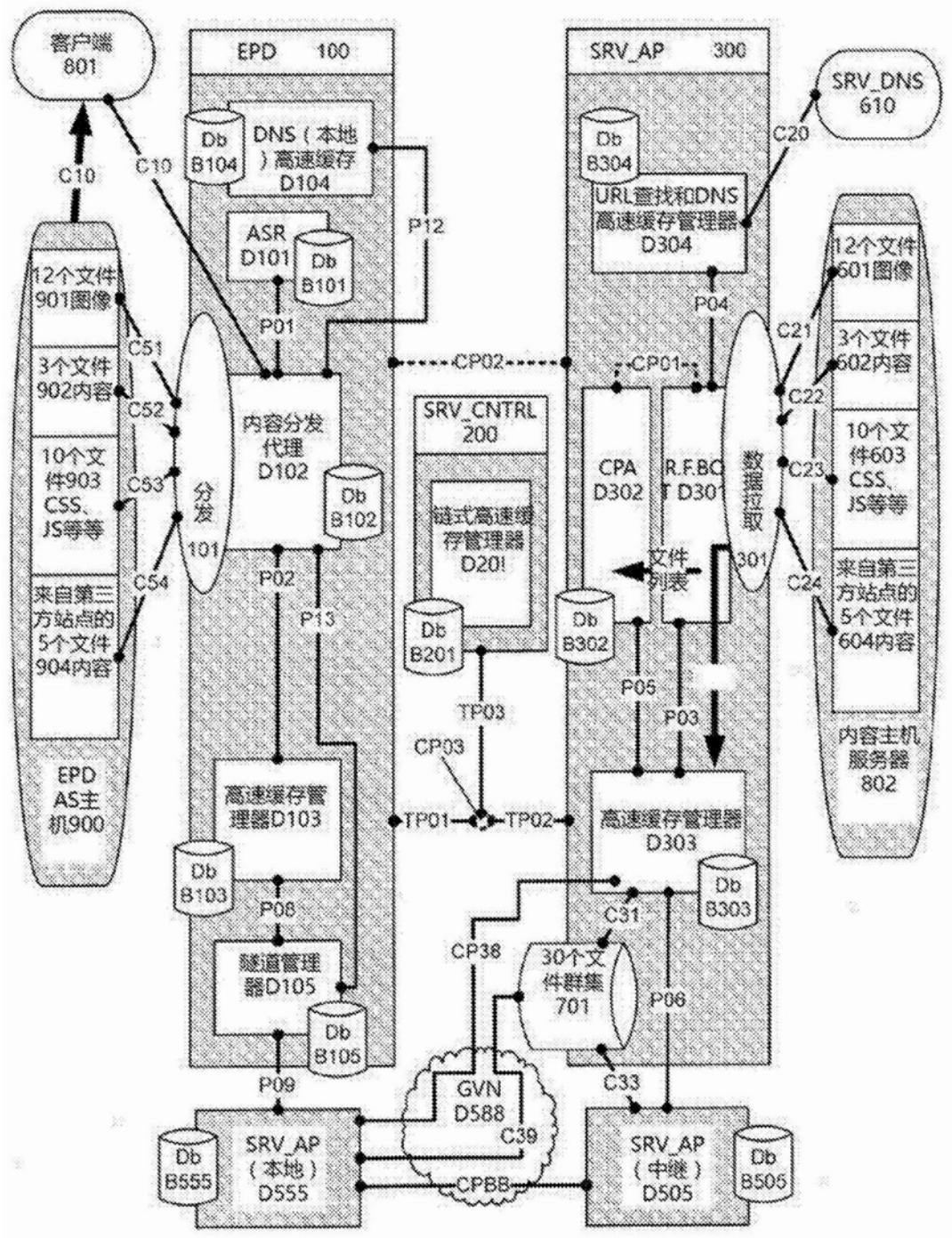

客户端
801
EPD 100
SRV_AP 300
SRV_DNS
610
C10
C10
Db
B104
DNS（本地）高速缓存
D104
Db
B304
C20
URL查找和DNS
高速缓存管理器
D304
ASR
D101
Db
B101
P12
P04
12个文件
901图像
3个文件
902内容
10个文
件903
CSS、
JS等等
来自第三
方站点的
5个文件
904内容
EPD
AS主
机900
C51
C52
C53
C54
P01
分发
101
内容分发
代理
D102
Db
B102
CP02
CP01
SRV_CNTRL
200
链式高速缓
存管理器
D201
Db
B201
CPA
D302
R.F.BC
T D301
数据过取
301
文件
列表
Db
B302
C21
C22
C23
C24
12个文件
601图像
3个文件
602内容
10个文
件603
CSS、
JS等等
来自第三
方站点的
5个文件
604内容
内容主机
服务器
802
P02
P13
P05
P03
TP03
CP03
TP01
TP02
高速缓存管理
器D103
高速缓存管理器
D303
Db
B103
Db
B303
P08
C31
CP38
隧道管理
器D105
30个文
件群集
701
P06
Db
B105
P09
C33
GVN
D588
C39
SRV_AP
（本地）
D555
SRV_AP
（中继）
D505
Db
B555
Db
B505
CPBB

图60

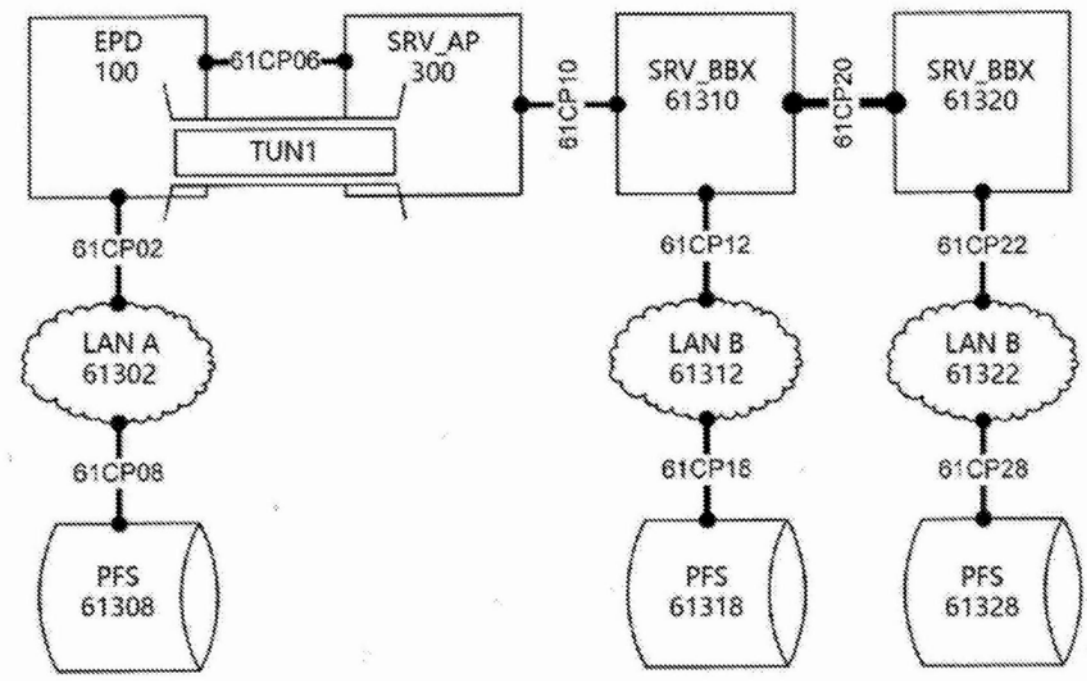

EPD
100
61CP06
SRV_AP
300
TUN1
61CP10
SRV_BBX
61310
61CP20
SRV_BBX
61320
61CP02
61CP12
61CP22
LAN A
61302
LAN B
61312
LAN B
61322
61CP08
61CP18
61CP28
PFS
61308
PFS
61318
PFS
61328

图61