(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2025 年 1 月 2 日 (02.01.2025)

WIPO | PCT

(10) 国际公布号
WO 2025/001981 A1

(51) 国际专利分类号:
H04W 48/08 (2009.01)

(21) 国际申请号: PCT/CN2024/100535

(22) 国际申请日: 2024 年 6 月 21 日 (21.06.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310793815.9 2023年6月29日 (29.06.2023) CN

(71) 申请人: 腾 讯 科 技 (深 圳) 有 限 公 司 **(TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED)** [CN/CN]; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。

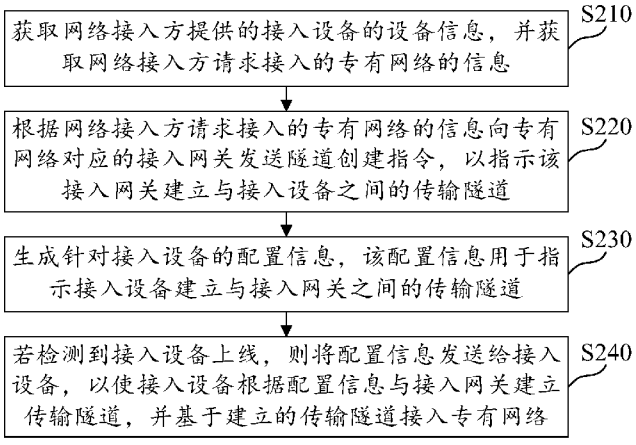
(72) 发明人: 刘国旭 **(LIU, Guoxu)**; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。

(74) 代理人: 北 京 德 琦 知 识 产 权 代 理 有 限 公 司 **(DEQI INTELLECTUAL PROPERTY LAW CORPORATION)**; 中国北京市海淀区知春路1号学院国际大厦7层, Beijing 100083 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(54) Title: ACCESS CONTROL METHOD AND APPARATUS, AND COMPUTER-READABLE MEDIUM AND ELECTRONIC DEVICE

(54) 发明名称: 接入控制方法、装置、计算机可读介质及电子设备



S210 Acquire device information of an access device, which device information is provided by a network accessing side, and acquire information of a private network that the network accessing side requests to access

S220 According to the information of the private network that the network accessing side requests to access, send a tunnel creation instruction to an access gateway corresponding to the private network, so as to instruct the access gateway to establish a transmission tunnel between the access gateway and the access device

S230 Generate configuration information for the access device, wherein the configuration information is used for instructing the access device to establish a transmission tunnel between the access device and the access gateway

S240 If it is detected that the access device gets online, send the configuration information to the access device, such that the access device establishes the transmission tunnel between the access device and the access gateway according to the configuration information, and accesses the private network on the basis of the established transmission tunnel

图 2

(57) Abstract: An access control method and apparatus, and a computer-readable medium and an electronic device. The access control method comprises: acquiring device information of an access device, and acquiring information of a private network that a network accessing side requests to access; sending a tunnel creation instruction to an access gateway corresponding to the private network, so as to instruct the access gateway to establish a transmission tunnel between the access gateway and the access device; generating configuration information for the access device, wherein the configuration information is used for instructing the access device to establish a transmission tunnel between the access device and the access gateway; and if it is detected that the access device gets online, sending the configuration information to the access device, such that the access device establishes the transmission tunnel between the access device and the access gateway according to the configuration information, and accesses the private network on the basis of the established transmission tunnel.

WO 2025/001981 A1

[见续页]

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 一种接入控制方法、装置、计算机可读介质及电子设备。该接入控制方法包括：获取接入设备的设备信息，并获取网络接入方请求接入的专有网络的信息；向专有网络对应的接入网关发送隧道创建指令，以指示接入网关建立与接入设备之间的传输隧道；生成针对接入设备的配置信息，所述配置信息用于指示接入设备建立与所述接入网关之间的传输隧道；若检测到所述接入设备上线，则将所述配置信息发送给所述接入设备，以使所述接入设备根据所述配置信息与所述接入网关建立传输隧道，并基于建立的传输隧道接入所述专有网络。

接入控制方法、装置、计算机可读介质及电子设备

本申请要求于2023年06月29日提交中国专利局、申请号为202310793815.9，发明名称为“接入控制方法、装置、计算机可读介质及电子设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及计算机及通信技术领域，具体而言，涉及一种接入控制方法、装置、计算机可读介质及电子设备。

背景技术

虚拟私有云（Virtual Private Cloud）是云用户在云上申请的隔离的、私密的虚拟网络环境。VPC通过子网将资源进行逻辑隔离为用户提供隔离的网络环境、灵活的可定义子网网段，并支持随时在现有VPC中追加新的定义网段，保证IP地址取之不尽，解决传统子网带来的节点数量的限制，同时云用户可以使用VPN等方式连接本地数据中心后将业务平滑迁移到云端。

技术内容

本申请的实施例提供了一种接入控制方法、装置、计算机可读介质及电子设备，可以降低接入专有网络时对传统专线网络的依赖，有效提高了网络接入速度。

本申请的其他特性和优点将通过下面的详细描述变得显然，或部分地通过本申请的实践而习得。

本申请实施例提供了一种接入控制方法，包括：获取接入设备的设备信息，并获取所述接入设备待接入的专有网络的信息；根据所述专有网络的信息向所述专有网络对应的接入网关发送隧道创建指令，以指示所述接入网关建立与所述接入设备之间的传输隧道；生成针对所述接入设备的配置信息，所述配置信息用于指示所述接入设备建立与所述接入网关之间的传输隧道；响应于检测到所述接入设备上线，则将所述配置信息发送给所述接入设备，以使所述接入设备根据所述配置信息与所述接入网关建立传输隧道，并基于建立的传输隧道接入所述专有网络。

本申请实施例还提供了一种接入控制装置，包括：获取单元，配置为获取接入设备的设备信息，并获取所述接入设备待接入的专有网络的信息；发送单元，配置为根据所

述专有网络的信息向所述专有网络对应的接入网关发送隧道创建指令，以指示所述接入网关建立与所述接入设备之间的传输隧道；生成单元，配置为生成针对所述接入设备的配置信息，所述配置信息用于指示所述接入设备建立与所述接入网关之间的传输隧道；处理单元，配置为响应于检测到所述接入设备上线，则将所述配置信息发送给所述接入设备，以使所述接入设备根据所述配置信息与所述接入网关建立传输隧道，并基于建立的传输隧道接入所述专有网络。

本申请实施例还提供了一种计算机可读介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如上述实施例中所述的接入控制方法。

本申请实施例还提供了一种电子设备，包括：一个或多个处理器；存储装置，用于存储一个或多个计算机程序，当所述一个或多个计算机程序被所述一个或多个处理器执行时，使得所述电子设备实现如上述实施例中所述的接入控制方法。

本申请实施例还提供了一种计算机程序产品，该计算机程序产品包括计算机程序，该计算机程序存储在计算机可读存储介质中。电子设备的处理器从计算机可读存储介质读取并执行该计算机程序，使得该电子设备执行上述各种可选实施例中提供的接入控制方法。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本申请。

附图简要说明

图 1 示出了可以应用本申请实施例的技术方案的示例性系统架构的示意图；

图 2 示出了根据本申请实施例的接入控制方法的流程图；

图 3 示出了可以应用本申请实施例的接入控制方案的示例性系统架构的示意图；

图 4 示出了可以应用本申请实施例的接入控制方案的示例性系统架构的示意图；

图 5 示出了根据本申请实施例的 CPE 与接入网关之间的连接关系示意图；

图 6 示出了可以应用本申请实施例的接入控制方案的示例性系统架构的示意图；

图 7 示出了根据本申请实施例的 UPF 与接入网关之间的连接关系示意图；

图 8 示出了根据本申请实施例的接入网关与专线网关之间的连接关系示意图；

图 9 示出了根据本申请实施例的接入控制方法的交互流程图；

图 10 示出了根据本申请实施例的云网络控制器根据心跳消息进行处理的示意图；

图 11 示出了根据本申请实施例的接入控制方法的交互流程图；

图 12 示出了根据本申请实施例的接入控制装置的框图；

图 13 示出了适于用来实现本申请实施例的电子设备的计算机系统的结构示意图。

具体实施方式

现在参考附图以更全面的方式描述示例实施方式。然而，示例的实施方式能够以各种形式实施，且不应被理解为仅限于这些范例；相反，提供这些实施方式的目的是使得本申请更加全面和完整，并将示例实施方式的构思全面地传达给本领域的技术人员。

此外，本申请所描述的特征、结构或特性可以以任何合适的方式结合在一个或更多实施例中。在下面的描述中，有许多具体细节从而可以充分理解本申请的实施例。然而，本领域技术人员应意识到，在实施本申请的技术方案时可以不需用到实施例中的所有细节特征，可以省略一个或更多特定细节，或者可以采用其它的方法、元件、装置、步骤等。

附图中所示的方框图仅仅是功能实体，不一定必须与物理上独立的实体相对应。即，可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

附图中所示的流程图仅是示例性说明，不是必须包括所有的内容和操作/步骤，也不是必须按所描述的顺序执行。例如，有的操作/步骤还可以分解，而有的操作/步骤可以合并或部分合并，因此实际执行的顺序有可能根据实际情况改变。

需要说明的是：在本文中提及的“多个”是指两个或两个以上。“和/或”描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B 可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。字符“/”一般表示前后关联对象是一种“或”的关系。

本申请实施例的技术方案涉及到云技术（Cloud technology）领域，其中，云技术是指在广域网或局域网内将硬件、软件、网络等系列资源统一起来，实现数据的计算、储存、处理和共享的一种托管技术。

云技术是基于云计算商业模式应用的网络技术、信息技术、整合技术、管理平台技术、应用技术等的总称，可以组成资源池，按需所用，灵活便利。云技术网络系统的后台服务需要大量的计算、存储资源，如视频网站、图片类网站和更多的门户网站。伴随着互联网行业的高度发展和应用，将来每个物品都有可能存在自己的识别标志，都需要传输到后台系统进行逻辑处理，不同程度级别的数据将会分开处理，各类行业数据皆需

要强大的系统后盾支撑，只能通过云计算来实现。

在一些实施方法中，云用户如果想将本地 IDC（Internet Data Center，互联网数据中心）或网络设备与云端的 VPC（Virtual Private Cloud，虚拟私有云，也称为专有网络）打通，且享有低时延、高带宽、安全的网络质量，只能通过运营商开通专线的方式接入本地运营商最近的 POP（Point-of-Presence，入网点）点，然后通过运营商专线连接至云 VPC。这种方式不仅成本高，而且专线开通时间受运营商施工影响，同时对于经常移动或需要多地点部署的用户来讲非常不方便。

本申请实施例提出了一种新的网络接入控制方案，可以通过控制设备（下文用“控制器”表示）下发隧道创建指令及配置信息的方式实现网络接入方对专有网络的接入，降低了接入专有网络时对传统专线网络的依赖，同时使得在接入设备上线之后，可以自动根据配置信息接入专有网络，有效提高了网络接入速度。

具体地，在本申请的一个具体应用场景中，如图 1 所示，系统架构包括控制器 101、网络接入方 102、移动网络核心网网元 103、专有网络 106，以及对应于专有网络 106 的接入网关（GateWay，简称 GW）104 和转发设备 105，网络接入方 102 内部署有至少一个接入设备 1021。

在一些实施例中，控制器 101 可以是服务器，该服务器可以是独立的物理服务器，也可以是多个物理服务器构成的服务器集群或者分布式系统，还可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、CDN（Content Delivery Network，内容分发网络）、以及大数据和人工智能平台等基础云计算服务的云服务器。接入设备 1021 可以是本地 CPE（Customer premises equipment，用户驻地设备）或者能够接入网络的终端设备等，终端设备比如可以是智能手机、平板电脑、笔记本电脑、台式计算机、智能音箱、智能手表、车载终端、飞行器等，但并不局限于此。

在本申请的一些实施例中，控制器 101 可以获取网络接入方 102 提供的接入设备 1021 的设备信息，并获取网络接入方 102 请求接入的专有网络（即接入设备 1021 待接入的专有网络）的信息。接入设备 1021 的设备信息比如可以是设备唯一标识、设备的网络地址、设备的端口信息等；专有网络的信息比如可以是专有网络的标识信息、网络地址信息、端口信息等。

在本申请的一些实施例中，控制器 101 在获取网络接入方 102 请求接入的专有网络的信息之后，根据专有网络的信息向专有网络对应的接入网关 104 发送隧道创建指令，

以指示接入网关 104 建立与接入设备 1021 之间的传输隧道。同时，控制器 101 可以生成针对接入设备 1021 的配置信息，该配置信息用于指示接入设备 1021 建立与接入网关 104 之间的传输隧道，进而控制器 101 在检测到接入设备 1021 上线之后，可以将该配置信息发送给接入设备 1021，以使接入设备 1021 根据该配置信息与接入网关 104 建立传输隧道，并基于建立的传输隧道接入专有网络。

在一些实施例中，由于接入设备 1021 与接入网关 104 之间的传输隧道是通过移动网络核心网网元 103 建立的，因此控制器 101 可以向接入网关 104 和核心网网元 103 发送通用路由封装（Generic Routing Encapsulation，简称 GRE）隧道建立指令，以指示核心网网元 103 与接入网关 104 建立 GRE 隧道；而接入设备 1021 与接入网关 104 之间建立的传输隧道可以承载在 GRE 隧道之上。

在一些实施例中，控制器 101 还可以向接入网关 104，以及连接在接入网关 104 和专有网络之间的转发设备 105 发送隧道创建指令，以指示接入网关 104 与转发设备 105 之间建立传输隧道，接入网关 104 与转发设备 105 之间的传输隧道用于将接入设备 1021 的流量传输至转发设备 105，以使转发设备 105 将接入设备 1021 的流量路由至专有网络。

在一些实施例中，为了保证数据的安全性，接入设备 1021 与接入网关 104 之间建立的传输隧道可以是 IPSec（Internet Protocol Security，互联网安全协议）隧道。在一些实施例中，由于接入网关 104 与转发设备 105 可以是部署在网络提供方内部的，因此不需要进行加密传输，所以在接入网关 104 上可以解封装 IPSec 隧道，然后将用户流量转入更为轻量的 VXLAN（Virtual Extensible Local Area Network，虚拟扩展局域网）隧道中，即接入网关 104 与转发设备 105 之间的传输隧道可以是 VXLAN 隧道。

在一些实施例中，核心网网元 103 可以是 UPF（User Plane Function，用户面功能），UPF 是 3GPP 5G 核心网系统架构的重要组成部分，主要负责 5G 核心网中用户平面数据包的路由和转发相关功能。转发设备 105 可以是 NGW（Next Generation GateWay，下一代网关），主要用于混合云专线接入、域间互通、公有云互通等场景，实现高性能转发，支持多租户接入，支持 TGRE（Tunnel-GRE）、VXLAN 隧道协议等，同时支持分片、重组、限速等特性。

在图 1 所示的系统架构中，通过控制器 101 下发隧道创建指令及配置信息的方式就可以实现接入设备对专有网络的接入，降低了接入专有网络时对传统专线网络的依赖，同时使得在接入设备上线之后，可以自动根据配置信息接入专有网络，有效提高了网络接入速度。

以下对本申请实施例的技术方案的实现细节进行详细阐述：

图 2 示出了根据本申请的一些实施例的接入控制方法的流程图，该接入控制方法可以由控制器来执行，该控制器可以是图 1 中所示的控制器 101。参照图 2 所示，该接入控制方法至少包括 S210 至 S230，详细介绍如下：

在 S210 中，获取网络接入方提供的接入设备的设备信息，并获取网络接入方请求接入的专有网络的信息。

在一些实施例中，网络接入方可以通过配置接口或者控制台等向控制器发送接入设备的设备信息，以及请求接入的专有网络的信息。网络接入方可以是专有网络的租用方，接入设备可以是 CPE 或者能够接入网络的终端设备等。接入设备 1021 的设备信息比如可以是设备唯一标识、设备的网络地址、设备的端口信息等；专有网络的信息比如可以是专有网络的标识信息、网络地址信息、端口信息等。

在 S220 中，根据网络接入方请求接入的专有网络的信息向专有网络对应的接入网关发送隧道创建指令，以指示该接入网关建立与接入设备之间的传输隧道。

在一些实施例中，接入网关与接入设备之间的传输隧道可以是 IPSec 隧道，这样使得接入设备的数据在传输至接入网关的过程中，能够保证数据的安全性。在这种情况下，控制器可以获取网络接入方针对接入设备提供的隧道加密密钥，然后在隧道创建指令中添加该隧道加密密钥，以使接入设备与接入网网关之间基于隧道加密密钥建立加密传输隧道。

在一些实施例中，控制器向专有网络对应的接入网关发送隧道创建指令的过程具体可以是依次执行以下过程：向接入网关发送创建 VRF（Virtual Routing Forwarding，虚拟路由转发）信息、向接入网关发送创建 IPSec 隧道信息、向接入网关发送创建接口 IP 信息、向接入网关配置 IKE（一种混合型加密协议）加密信息、向接入网关配置 BGP（Border Gateway Protocol，边界网关协议）信息等。

在 S230 中，生成针对接入设备的配置信息，该配置信息用于指示接入设备建立与接入网关之间的传输隧道。

在一些实施例中，针对接入设备的配置信息可以包括：创建 IPSec 隧道信息、创建接口 IP 信息、配置的 IKE 加密信息。控制器生成针对节加入设备的配置信息之后，可以将该配置信息存储到数据库中。

需要说明的是，图 2 中所示的 S220 与 S230 之间的执行顺序并不做具体限定，比如可以按照图 2 中所示的顺序先执行 S220，再执行 S230；或者也可以先执行 S230，再执

行 S220；也可以同时执行 S220 与 S230。

在 S240 中，响应于检测到接入设备上线，则将配置信息发送给接入设备，以使接入设备根据配置信息与接入网关建立传输隧道，并基于建立的传输隧道接入专有网络。

在一些实施例中，接入设备在上线后可以向控制器周期性地发送心跳消息，那么控制器可以在接收到接入设备发送的心跳消息时，确定检测到接入设备上线。这样使得接入设备在上线之后，控制器就可以直接将配置信息发送给接入设备，进而接入设备可以自动与接入网关建立传输隧道。另外，接入设备接收到配置信息后，还可以在本地存储该配置信息。

在一些实施例中，接入设备上线后周期性发送的心跳消息中还可以包含有接入设备的上一次启动时间，那么控制器可以从接入设备发送的心跳消息中获取到接入设备的上一次启动时间，也可以从数据库中获取针对接入设备记录的上一次启动时间；如果心跳消息中包含的上一次启动时间与数据库中记录的上一次启动时间不一致，则说明接入设备发生了重启，那么可以获取接入设备中存储的当前配置信息。响应于接入设备的当前配置信息与数据库中存储的针对接入设备的配置信息不匹配，则可以将数据库中存储的配置信息发送给接入设备。该实施例的技术方案使得接入设备在重启后或者在本地存储的配置信息丢失的情况下，控制器可以及时将数据库中存储的针对接入设备的配置信息下发给接入设备，以保证接入设备能够获取到最新的配置信息，并基于最新的配置信息与接入网关建立传输隧道。

在一些实施例中，控制器将数据库中存储的针对接入设备的配置信息发送给接入设备的过程具体可以是：在数据库中存储的针对接入设备的配置信息中查找与当前配置信息存在差异的配置信息，然后将查找到的存在差异的配置信息发送给接入设备。该实施例的技术方案使得可以仅向接入设备发送差异配置信息，相较于向接入设备发送完整配置信息，可以减少发送配置信息所占用的带宽和传输时间，进而确保接入设备能够尽快获取到最新的配置信息。

在一些实施例中，控制器在将差异配置信息发送给接入设备之后，可以根据心跳消息中包含的上一次启动时间，对数据库中针对接入设备记录的上一次启动时间进行更新，以便于后续根据数据库中更新后的上一次启动时间来确定接入设备是否发生了重启。

在一些实施例中，专有网络可以对应有至少两个接入网关，那么控制器可以将配置信息发送给接入设备，以指示接入设备分别与至少两个接入网关建立传输隧道，并指示接入设备将接入设备与至少两个接入网关之间建立的传输隧道配置为等价多径路由

（Equal Cost Multi-path，简称 ECMP）的方式，进而可以在任一接入网关出现故障时，能够通过其它接入网关无缝实现业务流量的接替，保证了业务流量传输的持续性与稳定性。

在一些实施例中，接入设备与接入网元之间的传输隧道可以是接入设备通过核心网网元与接入网关建立的，在这种情况下，控制器可以向接入网关和核心网网元发送 GRE 隧道建立指令，以指示核心网网元与接入网关建立 GRE 隧道；在这种情况下，接入设备与接入网关之间的传输隧道可以承载在 GRE 隧道之上。比如，接入设备与接入网关之间的传输隧道为 IPSec 隧道，那么在接入设备与接入网关之间建立的传输隧道中，核心网网元与接入网关之间的传输隧道为 IPSec over GRE 隧道。

在一些实施例中，专有网络可以对应有至少两个接入网关，在这种情况下，控制器可以向至少两个接入网关和至少两个核心网网元发送 GRE 隧道建立指令，以指示每个核心网网元分别与至少两个接入网关建立 GRE 隧道，并指示每个核心网网元将该核心网网元与至少两个接入网关之间建立的 GRE 隧道配置为等价多径路由的方式。该实施例的技术方案使得可以高效利用接入网关和核心网网元之间的转发能力，并且也可以在部分核心网网元或者部分接入网关出现异常中，通过 ECMP 来保证网络传输的可靠性和稳定性。

在一些实施例中，接入网关与专有网络之间可以连接有转发设备，转发设备可以是网关设备，比如转发设备可以是 NGW 设备，转发设备可以在接收到接入网关转发过来的用户流量之后，将用户流量转发到专有网络中。

在一些实施例中，控制器可以向接入网关，以及连接在接入网关和专有网络之间的转发设备发送隧道创建指令，以指示接入网关与转发设备之间建立传输隧道，接入网关与转发设备之间的传输隧道用于将接入设备的流量传输至转发设备，以使转发设备将接入设备的流量路由至专有网络。

在一些实施例中，专有网络可以对应于至少两个接入网关和至少两个转发设备，那么控制器可以向至少两个接入网关和至少两个转发设备发送隧道创建指令，以指示每个接入网关分别与至少两个转发设备之间建立传输隧道，并指示每个接入网关将该接入网关与至少两个转发设备之间建立的传输隧道配置为等价多径路由的方式。该实施例的技术方案使得可以高效利用接入网关和转发设备之间的转发能力，并且也可以在部分转发设备或者部分接入网关出现异常中，通过 ECMP 来保证网络传输的可靠性和稳定性。

在一些实施例中，由于接入网关与转发设备是在网络提供方内部，因此不需要进行加密传输，故接入网关与转发设备之间的传输隧道可以是轻量级的 VXLAN 隧道。如果接

入设备与接入网关之间的传输隧道是IPSec隧道,那么接入网关可以解封装IPSec隧道,然后将用户流量转入VXLAN隧道中,进而路由至转发设备,由转发设备传输给专有网络。

本申请上述实施例的技术方案中通过根据接入设备待接入的专有网络的信息向专有网络对应的接入网关发送隧道创建指令，以指示该接入网关建立与接入设备之间的传输隧道；同时生成针对接入设备的配置信息，以在检测到接入设备上线之后，将该配置信息发送给接入设备，以使接入设备根据该配置信息与接入网关建立传输隧道，并基于建立的传输隧道接入专有网络，使得可以通过（控制器）下发隧道创建指令及配置信息的方式就可以实现接入设备对专有网络的接入，降低了接入专有网络时对传统专线网络的依赖，同时使得在接入设备上线之后，可以自动根据配置信息接入专有网络，有效提高了网络接入速度。

以下结合图 3 至图 11，以具体的应用场景对本申请实施例的网络接入方案再次进行详细说明：

在图3所示的应用场景中,云网络控制器用于实现前述实施例中所述的控制器的功能。其中，用户侧可以是租用专有网络 VPC 的用户，也即前述实施例中的网络接入方、UPF 即为前述实施例中的核心网网元、专线网关即为前述实施例中的转发设备。图 3 所示实施例的技术方案主要采用 NFV（Network Functions Virtualization，网络功能虚拟化）中转控分离的设计思路，分为云上部署的云网络控制器和下层的网络设备。云网络控制器负责对设备的管控、配置下发、状态检测等，网络设备包括用户侧的用于接入网络的移动 CPE；运营商侧的基站、UPF 等；云提供商侧的接入网关、专线网关等。

基于图3所示的应用场景，当用户侧的CPE设备接入网络时，用户侧可以将自己的CPE设备（或CPE下面挂载的私有IDC机房）接入离用户侧最近的网络，比如可以是移动网络，具体可以是4G或5G网络等。运营商侧的UPF与云提供商侧的接入网关之间可以通过专线连接。

由于空口网络是承载在公网之上,所以用户数据需要考虑加密性,因此如图4所示,可以在用户CPE设备与接入网关之间可以采用IPSec隧道方式，加密隧道直接穿过运营商网络抵达接入网关，使运营商公网和内网链路感知不到隧道，能够最大程度保证用户数据的安全性。

在一些实施例中，在云提供商网络中，为了网络的可靠性，可能会部署两台（或多台）双主模式的接入网关。两台接入网关同时工作，各自负载一部分的网络流量，任何一台出现故障时，另一台无需切换即可承接所有业务流量。如图5所示，用户CPE可以

与两台接网关都建立 IPSec 隧道，且在 CPE 上配置 ECMP 使两条 IPSec 隧道等价路由。隧道建立和故障链路切换的过程都是网络设备自动完成的，用户完全不感知，能够给用户提供良好的体验。

在一些实施例中，如图 6 所示，在云提供商与运营商网络的连接中，运营商通常会提供通用的 GRE 隧道来进行网络封装，用于区分其不同的用户。GRE 隧道的一端是运营商的 UPF，另一端是云厂商的接入网关，GRE 隧道用来承载用户 CPE 建立的 IPSec 隧道。此时，底层网络（underlay）的 GRE 隧道对于用户是不可见的，用户 CPE 所建立的 IPSec 隧道在通过 UFP 时会自动负载到 GRE 隧道上，即 IPSec over GRE 的形式接入云上的网关。

在一些实施例中，如图 7 所示，运营商通常会提供 2 台以上的 UPF（以下以 2 台为例进行说明）作为接入，此时可以通过云网络控制器对两台 UPF 和两台接入网关之间都建立全互联模式（full mesh）的 GRE 隧道，且在各自的设备上两条隧道为 ECMP。这样可以高效的利用网络设备的转发能力，也能在异常情况下保证网络的高可靠性和稳定性。比如一台 UPF 设备不可用，由于 ECMP 调度的特性，流量会经由另一台 UPF 转发，当异常设备恢复上线后，流量的分发也会自动恢复。接入网关也是同理，只要网络中至少还剩一台 UPF 和接入网关，用户的流量就不会受损，提高了链路质量的可用性。

在一些实施例中，当用户流量到达接入网关后，需要经由专线网关到达 VPC。在接入网关和专线网关之间可以采用 VXLAN 隧道，VXLAN 的 VNI（VXLAN Network Identifier，VXLAN 网络标识符）有 24 个 bit，最多可支持 1600w+的用户接入，远多于 VLAN（Virtual Local Area Network，虚拟局域网）的 12bit，因此 VXLAN 隧道十分适合云提供商接入时划分租户。又由于网络流量已经进入到云提供商内部，因此无需加密传输，故在接入网关上即可解封装 IPSec 隧道，将用户流量转入更为轻量的 VXLAN 隧道中。

在一些实施例中，如图 8 所示，云提供商可以提供 2 台以上的接入网关和专线网关（以下以 2 台为例进行说明）作为接入，此时可以通过云网络控制器对两台接入网关和两台专线网关之间都建立 VXLAN 隧道，且在各自的设备上的两条隧道为 ECMP。这样可以高效的利用网络设备的转发能力，也能在异常情况下保证网络的高可靠性和稳定性。

在本申请的一些实施例中，当用户购入一台 CPE 设备时，通过云网络控制器能够配置隧道将 CPE 设备接入云提供商，然后由云网络控制器编排网络隧道指令配置到两端设备上，CPE 设备即可完成接入。具体如图 9 所示，包括以下步骤：

S901，用户购入 CPE 设备后，通过云网络控制器开通 CPE 入云功能，并配置加密密

钥。

S902，云网络控制器开始编排该 CPE 接入的 IPSec 隧道，然后准备向 CPE 和接入网关发送创建隧道的指令。

之后，云网络控制器执行 S903a 至 S903e，即向接入网关依次发送创建 VRF 信息、创建 IPSec 隧道信息、创建接口 IP 信息，以及配置 IKE 加密信息、配置 BGP 信息等。然后，云网络控制器执行 S904a 至 S904c，即向 CPE 依次发送创建 IPSec 隧道信息、创建接口 IP 信息，以及配置 IKE 加密信息等。

当 CPE 和接入网关都配置完毕后，CPE 即可自动接入到接入网关，打通本地 IDC 与云上 VPC 网络。

在本申请的一些实施例中，由于用户 CPE 处于自己的网络环境中，不像接入网关作为服务器部署，因此云网络控制器编排的指令并不一定随时都能发送到 CPE 上（比如 CPE 可能未开机）。而用户通过云网络控制器配置之后期望 CPE 一旦上线即可自动接入专有网络，这就需要云网络控制器能够提供 CPE 状态检测和配置重下发功能。

可选地，每一台 CPE 在云网络控制器的数据库表中都可以存有一条记录，如表 1 所示，可以记录 CPE 的标识信息、配置信息，此外还额外存储了 CPE 的上一次启动时间。当 CPE 上线之后，可以周期性向云网络控制器上报心跳信息，消息体中携带 CPE 的上一次启动时间。

CPE_ID（CPE 标识）	CONFIG（配置信息）	LAST_BOOT_TIME（最近启动时间）
CPE001	CONFIG_VALUE	2023-4-1 12:00:00

表 1

云网络控制器收到 CPE 上报的心跳消息时，会检查心跳消息中的上一次启动时间是否与数据库中存储的上一次启动时间一致，如果有更新说明 CPE 发生过重启。在 CPE 重启期间有可能有新的配置信息，也有可能 CPE 发生故障导致本地存储的配置信息丢失，因此云网络控制器会在确定 CPE 发生过重启时对 CPE 进行配置核查。比如，云网络控制器可以通过 CPE 的管理接口获取 CPE 的当前配置信息，然后与数据库中的配置信息进行比较，并将差异配置信息下发到 CPE 上。这样对于新购买的设备，用户通过云网络控制器进行初次配置后，云网络控制器会在 CPE 上电自动接入时为它补齐配置信息，然后 CPE 就会自动与云提供商的专有网络建立加密隧道，这个过程用户无感知。而在 CPE 使用期间，任何时候的断电重启或意外宕机，云网络控制器都会自动对 CPE 的配置信息进行核

查修复。同时，云网络控制器也需要及时更新数据库中存储的上一次启动时间，如图 10 所示，CPE 周期性上报心跳消息给云网络控制器，然后云网络控制器据此更新数据库中存储的信息，比如上一次启动时间等。

基于前述的系统架构和相关的配置，本申请实施例中采用了转控分离的思想，即各种配置信息都是通过云网络控制器进行编排下发的，底层的网络设备无需关心业务，只需提供标准的控制接口，按照云网络控制器的编排指令配置网络即可。一个示意的处理流程如图 11 所示，包括如下步骤：

S1101，初始化时，云网络控制器向 UPF 和接入网关发送配置信息，具体是通过云网络控制器将运营商的 UPF 与云提供商的接入网关打通，即在 UPF 与接入网关之间建立 GRE 隧道。

S1102，当用户需要使用专有网络时，通过云控制台向云网络控制器配置自身的 CPE 希望接入的 VPC 网络。

S1103，控制器通过下发配置信息至接入网关和专线网关，以在接入网关与专线网关之间配置 VXLAN 隧道，来打通接入网关与专线网关之间的连接。

S1104，控制器为该用户分配专属的 IPSec 隧道资源，分配配置到 CPE 和接入网关上，以打通 CPE 与接入网关之间的连接。

在完成上述配置之后，用户即可通过 CPE 使用移动网络的方式接入到云上 VPC 中。

可见，在本申请的实施例中，用户 CPE 可以快速高效接入云 VPC，充分利用了 4G/5G 网络的低时延、高带宽特性，取代了一些实施方法中接入专有网关时对于传统专线的依赖。同时，通过云网络控制器，用户只需简单的配置即可让 CPE 设备自动接入专有网络，对于设备离线、异常宕机等场景，云网络控制器也能自动为其恢复。通过多台互为主备的云上网络设备，构建 full mesh 的网络隧道，提供可靠性更高的连接服务，给用户带来不亚于专线连接的网络质量。

以下介绍本申请的装置实施例，可以用于执行本申请上述实施例中的接入控制方法。对于本申请装置实施例中未披露的细节，请参照本申请上述的接入控制方法的实施例。

图 12 示出了根据本申请的一些实施例的接入控制装置的框图，该接入控制装置可以设置在控制器内。

参照图 12 所示，根据本申请的一些实施例的接入控制装置 1200，包括：获取单元 1202、发送单元 1204、生成单元 1206 和处理单元 1208。

其中，获取单元 1202 配置为获取接入设备的设备信息，并获取所述接入设备待接

入的专有网络的信息；发送单元 1204 配置为根据所述专有网络的信息向所述专有网络对应的接入网关发送隧道创建指令，以指示所述接入网关建立与所述接入设备之间的传输隧道；生成单元 1206 配置为生成针对所述接入设备的配置信息，所述配置信息用于指示所述接入设备建立与所述接入网关之间的传输隧道；处理单元 1208 配置为响应于检测到所述接入设备上线，则将所述配置信息发送给所述接入设备，以使所述接入设备根据所述配置信息与所述接入网关建立传输隧道，并基于建立的传输隧道接入所述专有网络。

在本申请的一些实施例中，基于前述方案，所述接入控制装置 1200 还包括：接收单元，配置为接收所述接入设备上线后周期性发送的心跳消息，所述心跳消息中包含有所述接入设备的上一次启动时间；所述获取单元 1202 还配置为：从数据库中获取针对所述接入设备记录的上一次启动时间；若所述心跳消息中包含的上一次启动时间与所述数据库中记录的上一次启动时间不一致，则获取所述接入设备中的当前配置信息；所述发送单元 1204 还配置为：响应于所述当前配置信息与所述数据库中存储的针对所述接入设备的配置信息不匹配，则将所述数据库中存储的针对所述接入设备的配置信息发送给所述接入设备。

图 13 示出了适于用来实现本申请实施例的电子设备的计算机系统的结构示意图，该电子设备可以是前述实施例中的控制器。

需要说明的是，图 13 示出的电子设备的计算机系统 1300 仅是一个示例，不应对本申请实施例的功能和使用范围带来任何限制。

如图 13 所示，计算机系统 1300 可以包括中央处理单元（Central Processing Unit，CPU）1301，其可以根据存储在只读存储器（Read-Only Memory，ROM）1302 中的程序或者从存储部分 1308 加载到随机访问存储器（Random Access Memory，RAM）1303 中的程序而执行各种适当的动作和处理，例如执行上述实施例中所述的方法。在 RAM 1303 中，还存储有系统操作所需的各种程序和数据。CPU 1301、ROM 1302 以及 RAM 1303 通过总线 1304 彼此相连。输入/输出（Input /Output，I/O）接口 1305 也连接至总线 1304。

以下部件可以连接至 I/O 接口 1305：包括键盘、鼠标等的输入部分 1306；包括诸如阴极射线管（Cathode Ray Tube，CRT）、液晶显示器（Liquid Crystal Display，LCD）等以及扬声器等的输出部分 1307；包括硬盘等的存储部分 1308；以及包括诸如 LAN（Local Area Network，局域网）卡、调制解调器等的网络接口卡的通信部分 1309。通信部分 1309 经由诸如因特网的网络执行通信处理。驱动器 1310 也根据需要连接至 I/O

接口 1305。可拆卸介质 1311，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器 1310 上，以便于从其上读出的计算机程序根据需要被安装入存储部分 1308。

特别地，根据本申请的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本申请的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序用于执行流程图所示的方法。在这样的实施例中，该计算机程序可以通过通信部分 1309 从网络上被下载和安装，和/或从可拆卸介质 1311 被安装。在该计算机程序被中央处理单元（CPU）1301 执行时，执行本申请的系统中限定的各种功能。

需要说明的是，本申请实施例所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（Erasable Programmable Read Only Memory，EPROM）、闪存、光纤、便携式紧凑磁盘只读存储器（Compact Disc Read-Only Memory，CD-ROM）、光存储器件、磁存储器件、或者上述的任意合适的组合。在本申请中，计算机可读存储介质可以是任何包含或存储计算机程序的有形介质，该计算机程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本申请中，计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的计算机程序。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的计算机程序可以用任何适当的介质传输，包括但不限于：无线、有线等等，或者上述的任意合适的组合。

附图中的流程图和框图，图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。其中，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示

的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机程序的组合来实现。

描述于本申请实施例中所涉及到的单元可以通过软件的方式实现，也可以通过硬件的方式来实现，所描述的单元也可以设置在处理器中。其中，这些单元的名称在某种情况下并不构成对该单元本身的限定。

本申请还提供了一种计算机可读介质，该计算机可读介质可以是上述实施例中描述的电子设备中所包含的；也可以是单独存在，而未装配入该电子设备中。上述计算机可读介质承载有一个或者多个计算机程序，当上述一个或者多个计算机程序被一个该电子设备执行时，使得该电子设备实现上述实施例中所述的方法。

应当注意，尽管在上文详细描述中提及了用于动作执行的设备的若干模块或者单元，但是这种划分并非强制性的。实际上，根据本申请的实施方式，上文描述的两个或更多模块或者单元的特征和功能可以在一个模块或者单元中具体化。反之，上文描述的一个模块或者单元的特征和功能可以进一步划分为由多个模块或者单元来具体化。

通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本申请实施方式的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中或网络上，包括若干指令以使得一台电子设备执行根据本申请实施方式的方法。

比如，电子设备可以是控制器，那么控制器可以执行图 2 所示的接入控制方法。

本领域技术人员在考虑说明书及实践这里公开的实施方式后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。

应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

权利要求书

1. 一种接入控制方法，由控制设备执行，所述方法包括：

获取接入设备的设备信息，并获取所述接入设备待接入的专有网络的信息；

根据所述专有网络的信息向所述专有网络对应的接入网关发送隧道创建指令，以指示所述接入网关建立与所述接入设备之间的传输隧道；

生成针对所述接入设备的配置信息，所述配置信息用于指示所述接入设备建立与所述接入网关之间的传输隧道；

响应于检测到所述接入设备上线，将所述配置信息发送给所述接入设备，以使所述接入设备根据所述配置信息与所述接入网关建立传输隧道，并基于建立的传输隧道接入所述专有网络。

2. 根据权利要求 1 所述的接入控制方法，其中，所述接入控制方法还包括：

响应于接收到所述接入设备发送的心跳消息，确定检测到所述接入设备上线；其中，所述心跳消息是所述接入设备上线后周期性发送的。

3. 根据权利要求 1 所述的接入控制方法，其中，生成针对所述接入设备的配置信息后，进一步包括：将所述配置信息存储到数据库中；

所述接入控制方法还包括：

接收所述接入设备上线后周期性发送的心跳消息，所述心跳消息中包含有所述接入设备的上一次启动时间；

从数据库中获取针对所述接入设备记录的上一次启动时间；

响应于所述心跳消息中包含的上一次启动时间与所述数据库中记录的上一次启动时间不一致，获取所述接入设备中的当前配置信息；

响应于所述当前配置信息与所述数据库中存储的针对所述接入设备的配置信息不匹配，将所述数据库中存储的配置信息发送给所述接入设备。

4. 根据权利要求 3 所述的接入控制方法，其中，将所述数据库中存储的配置信息发送给所述接入设备，包括：

在所述数据库中存储的针对所述接入设备的配置信息中查找与所述当前配置信息存在差异的配置信息；

将查找到的存在差异的配置信息发送给所述接入设备。

5. 根据权利要求 3 或 4 所述的接入控制方法，其中，在将所述数据库中存储的配置信息发送给所述接入设备之后，所述接入控制方法还包括：

根据所述心跳消息中包含的上一次启动时间，对所述数据库中针对所述接入设备记录的上一次启动时间进行更新。

6. 根据权利要求 1 至 5 任一项所述的接入控制方法，其中，所述接入控制方法还包括：

获取所述网络接入方针对所述接入设备提供的隧道加密密钥；

在所述隧道创建指令和所述配置信息中添加所述隧道加密密钥，以使所述接入设备与所述接入网关之间基于所述隧道加密密钥建立加密传输隧道。

7. 根据权利要求 1 至 6 任一项所述的接入控制方法，其中，所述传输隧道是所述接入设备通过核心网网元与所述接入网关建立的；所述接入控制方法还包括：

向所述接入网关和所述核心网网元发送通用路由封装 GRE 隧道建立指令，以指示所述核心网网元与所述接入网关建立 GRE 隧道；

其中，所述接入设备与所述接入网关之间建立的传输隧道承载在所述 GRE 隧道之上。

8. 根据权利要求 7 所述的接入控制方法，其特征在于，所述专有网络对应有至少两个接入网关；所述向所述接入网关和所述核心网网元发送通用路由封装 GRE 隧道建立指令，以指示所述核心网网元与所述接入网关建立 GRE 隧道，包括：

向所述至少两个接入网关和至少两个所述核心网网元发送所述 GRE 隧道建立指令，以指示每个所述核心网网元分别与所述至少两个接入网关建立所述 GRE 隧道，并指示每个所述核心网网元将相应核心网网元与所述至少两个接入网关之间建立的 GRE 隧道配置为等价多径路由的方式。

9. 根据权利要求 1 至 8 任一项所述的接入控制方法，其中，所述专有网络对应有至少两个接入网关；将所述配置信息发送给所述接入设备，以使所述接入设备根据所述配置信息与所述接入网关建立传输隧道，包括：

将所述配置信息发送给所述接入设备，以指示所述接入设备分别与所述至少两个接入网关建立传输隧道，并指示所述接入设备将所述接入设备与所述至少两个接入网关之间建立的传输隧道配置为等价多径路由的方式。

10. 根据权利要求 1 至 9 中任一项所述的接入控制方法，其中，所述接入控制方法还包括：

向所述接入网关，以及连接在所述接入网关和所述专有网络之间的转发设备发送隧道创建指令，以指示所述接入网关与所述转发设备之间建立传输隧道，所述接入网关与所述转发设备之间的传输隧道用于将所述接入设备的流量传输至所述转发设备，以使所

述转发设备将所述接入设备的流量路由至所述专有网络。

11. 根据权利要求 10 所述的接入控制方法，其中，所述专有网络对应于至少两个接入网关和至少两个转发设备；向所述接入网关，以及连接在所述接入网关和所述专有网络之间的转发设备发送隧道创建指令，以指示所述接入网关与所述转发设备之间建立传输隧道，包括：

向所述至少两个接入网关和至少两个转发设备发送隧道创建指令，以指示每个所述接入网关分别与所述至少两个转发设备之间建立传输隧道，并指示每个所述接入网关将相应接入网关与所述至少两个转发设备之间建立的传输隧道配置为等价多径路由的方式。

12. 根据权利要求 10 或 11 所述的接入控制方法，其中，所述接入设备与所述接入网关之间建立的传输隧道包括互联网安全协议隧道；所述接入网关与所述转发设备之间建立的传输隧道包括虚拟扩展局域网隧道，所述虚拟扩展局域网隧道用于将所述接入网关对所述互联网安全协议隧道解封装之后的流量传输至所述转发设备。

13. 一种接入控制装置，包括：

获取单元，配置为获取接入设备的设备信息，并获取所述接入设备待接入的专有网络的信息；

发送单元，配置为根据所述专有网络的信息向所述专有网络对应的接入网关发送隧道创建指令，以指示所述接入网关建立与所述接入设备之间的传输隧道；

生成单元，配置为生成针对所述接入设备的配置信息，所述配置信息用于指示所述接入设备建立与所述接入网关之间的传输隧道；

处理单元，配置为响应于检测到所述接入设备上线，则将所述配置信息发送给所述接入设备，以使所述接入设备根据所述配置信息与所述接入网关建立传输隧道，并基于建立的传输隧道接入所述专有网络。

14. 一种非易失性计算机可读介质，其上存储有计算机程序，其中，所述计算机程序被处理器执行时实现如权利要求 1 至 12 中任一项所述的接入控制方法。

15. 一种电子设备，包括：

一个或多个处理器；

存储器，用于存储一个或多个计算机程序，当所述一个或多个计算机程序被所述一个或多个处理器执行时，使得所述电子设备实现如权利要求 1 至 12 中任一项所述的接入控制方法。

16. 一种计算机程序产品，所述计算机程序产品包括计算机指令，所述计算机指令存储在计算机可读存储介质中，当所述计算机指令被执行时，实现如权利要求 1-12 中任一项所述的接入控制方法。

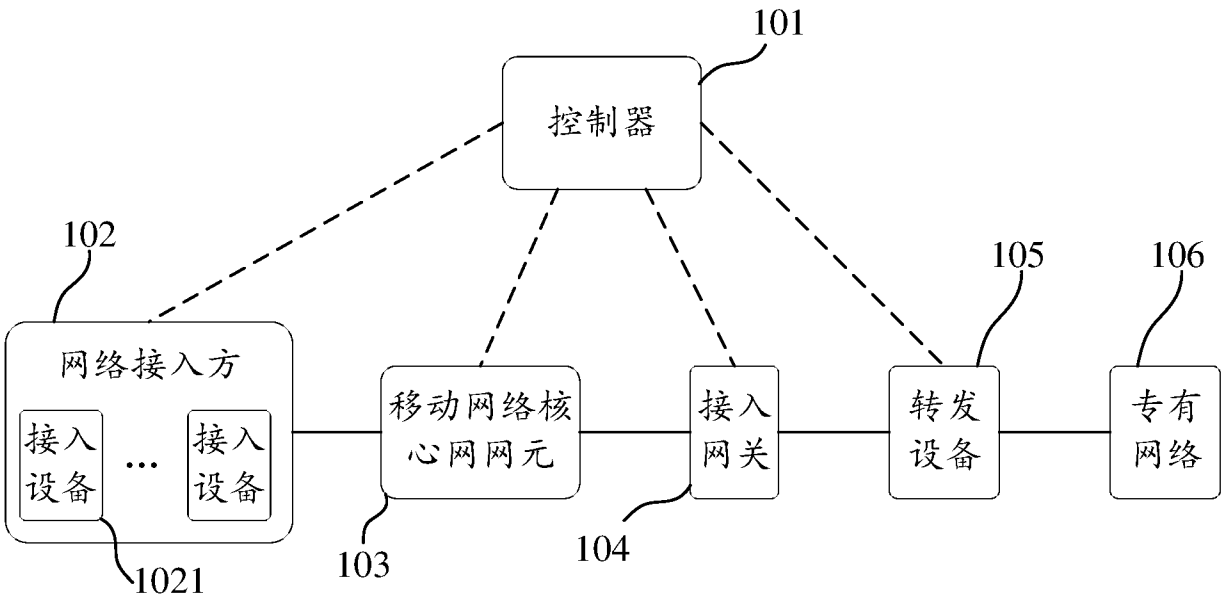

101
控制器
102
网络接入方
接入设备
...
接入设备
1021
103
移动网络核心网网元
104
接入网关
105
转发设备
106
专有网络

图 1

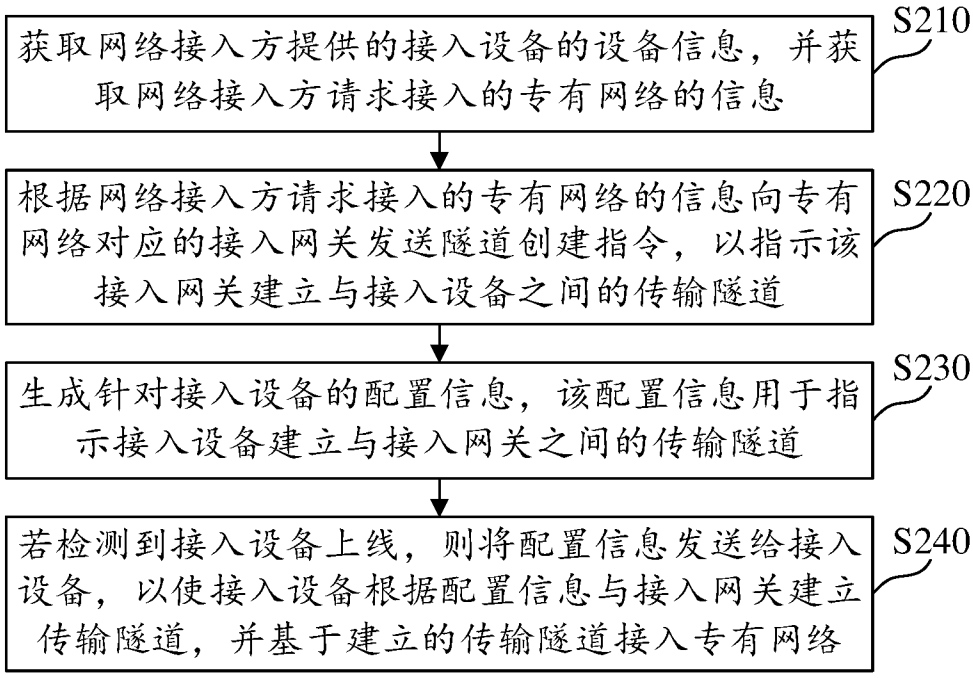

S210
获取网络接入方提供的接入设备的设备信息，并获取网络接入方请求接入的专有网络的信息
S220
根据网络接入方请求接入的专有网络的信息向专有网络对应的接入网关发送隧道创建指令，以指示该接入网关建立与接入设备之间的传输隧道
S230
生成针对接入设备的配置信息，该配置信息用于指示接入设备建立与接入网关之间的传输隧道
S240
若检测到接入设备上线，则将配置信息发送给接入设备，以使接入设备根据配置信息与接入网关建立传输隧道，并基于建立的传输隧道接入专有网络

图 2

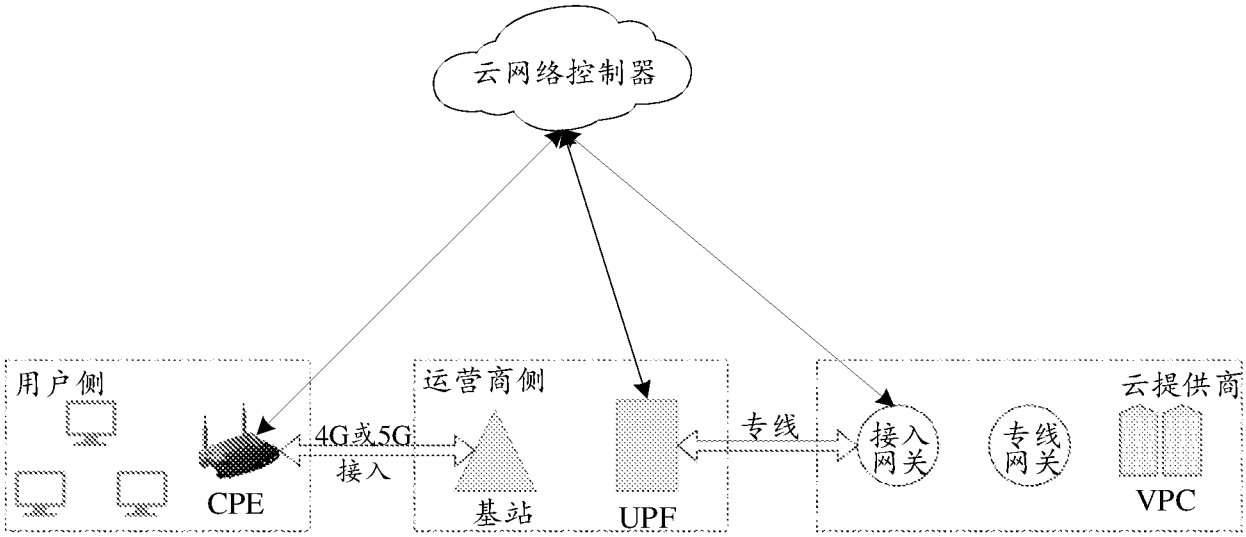

云网络控制器
用户侧
运营商侧
云提供商
4G或5G
接入
专线
接入网关
专线网关
CPE
基站
UPF
VPC

图 3

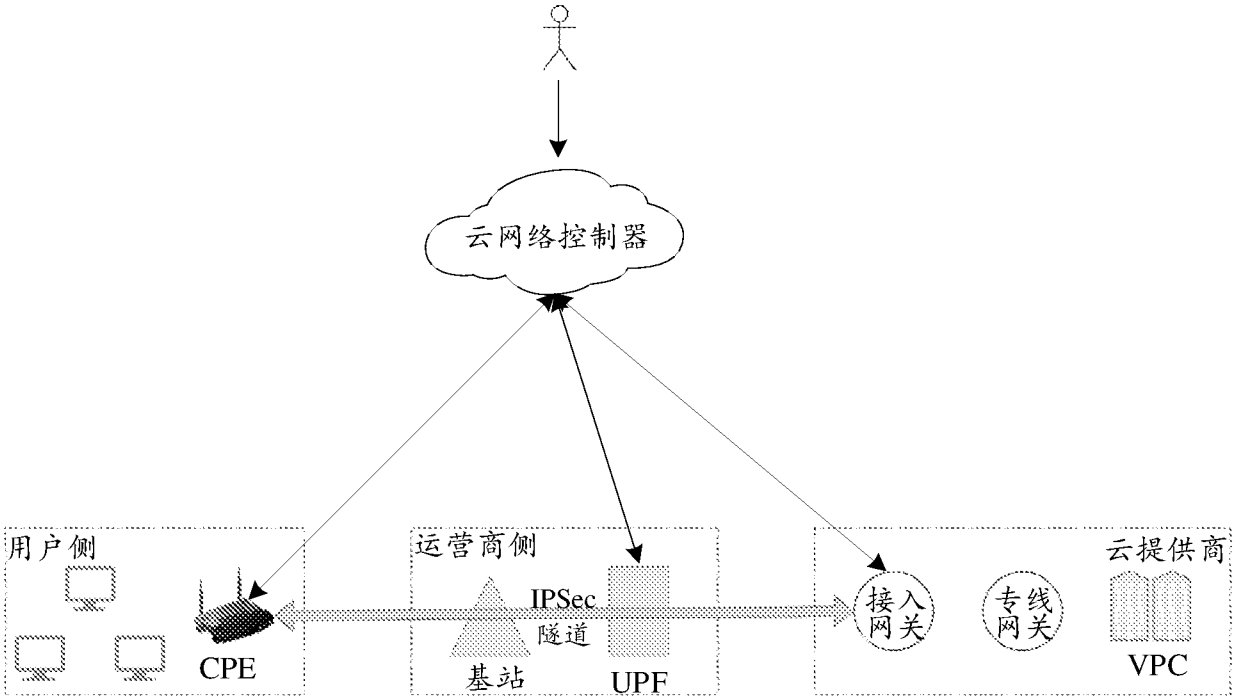

云网络控制器
用户侧
运营商侧
云提供商
IPSec
隧道
接入网关
专线网关
CPE
基站
UPF
VPC

图 4

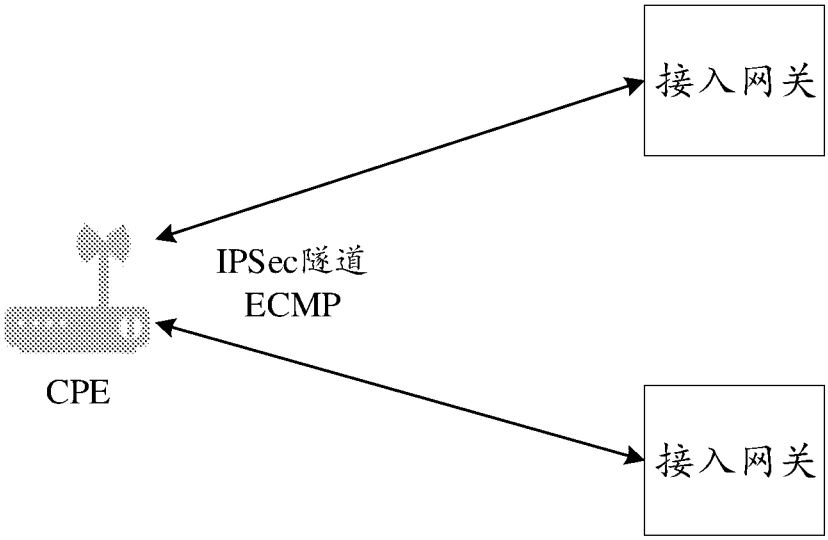

接入网关
IPSec隧道
ECMP
CPE
接入网关

图 5

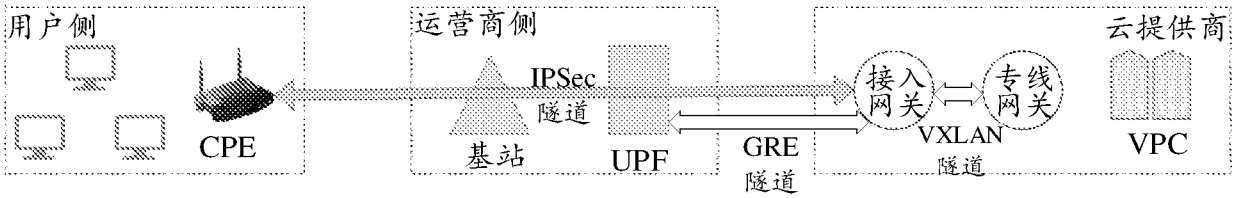

用户侧
CPE
运营商侧
IPSec
隧道
基站
UPF
GRE
隧道
接入
网关
专线
网关
VXLAN
隧道
云提供商
VPC

图 6

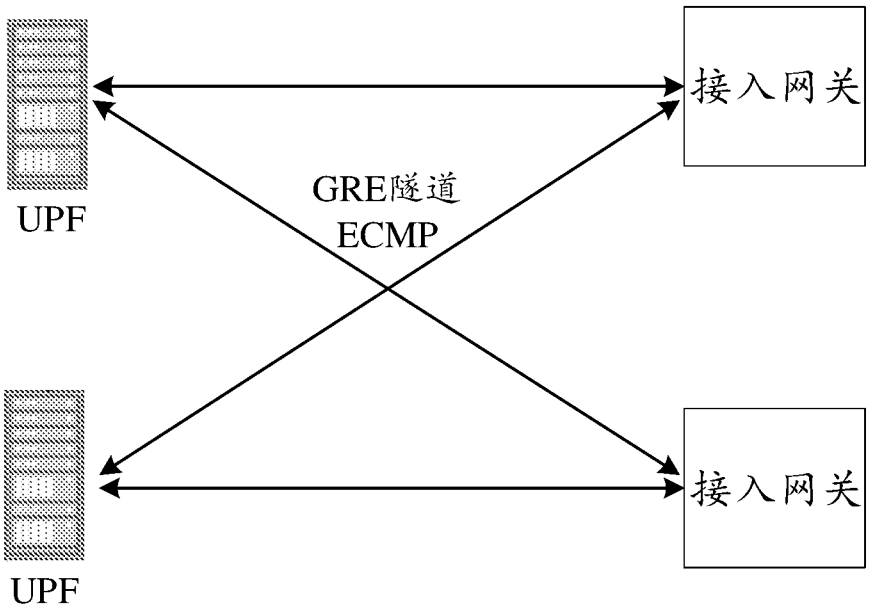

UPF
GRE隧道
ECMP
接入网关
UPF
接入网关

图 7

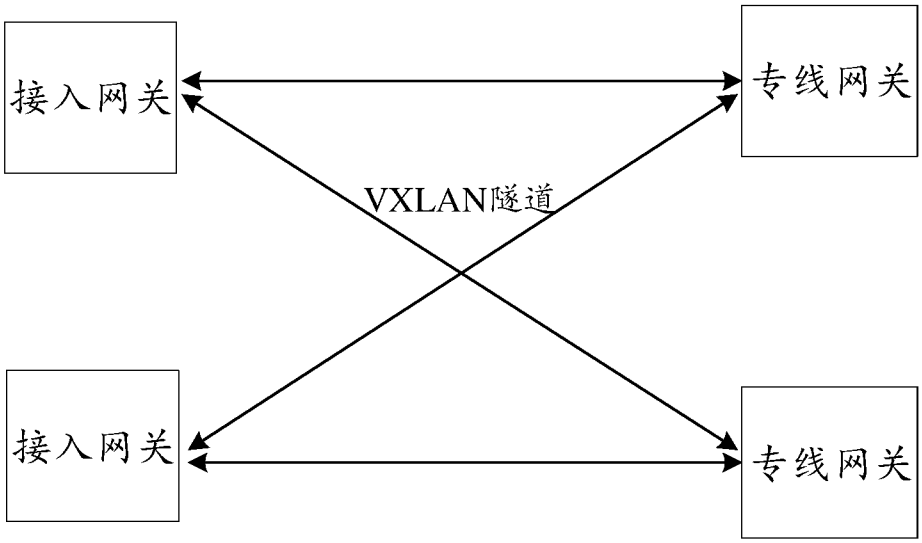

接入网关
专线网关
VXLAN隧道
接入网关
专线网关

图 8

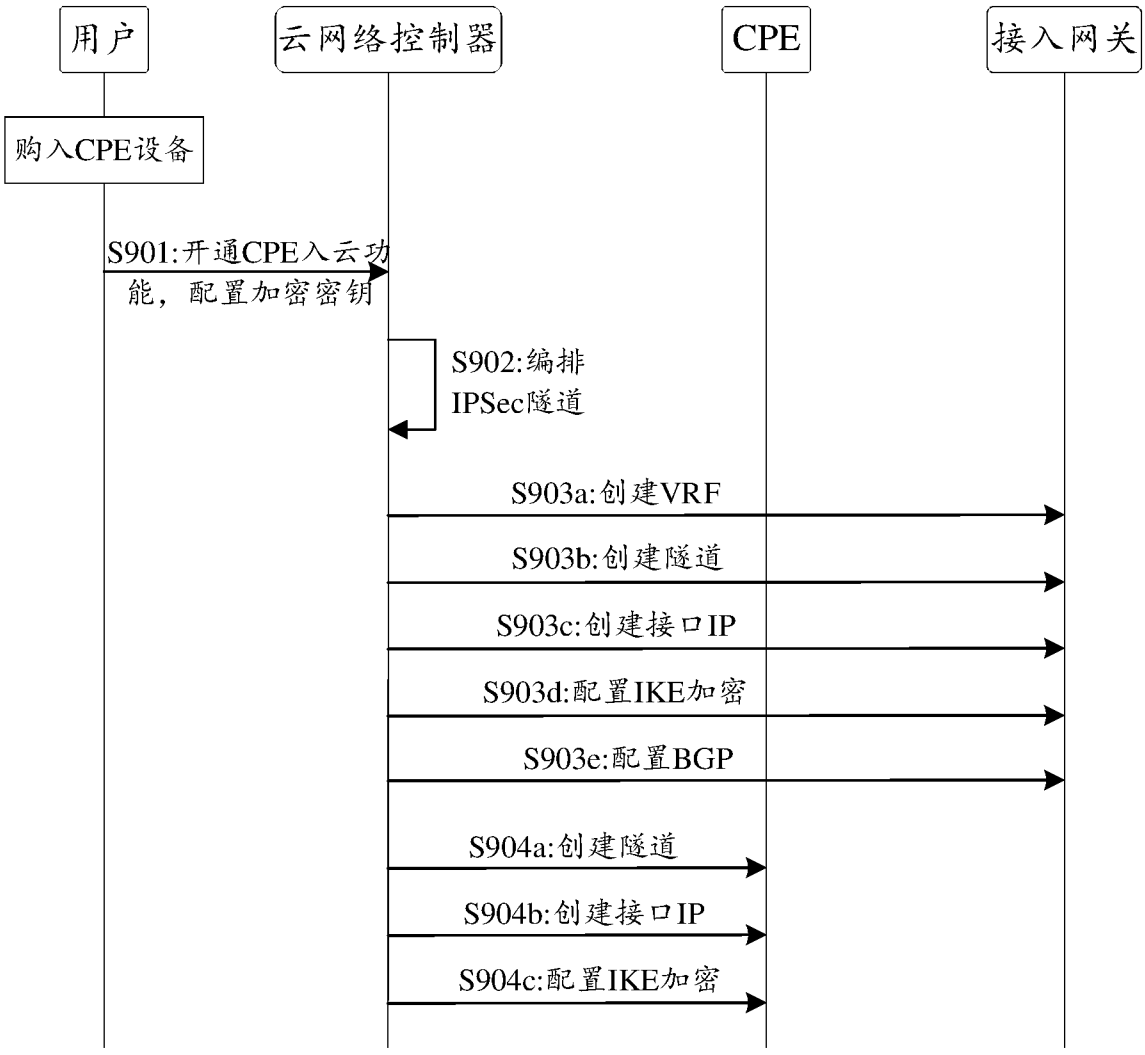

用户
云网络控制器
CPE
接入网关
购入CPE设备
S901:开通CPE入云功能，配置加密密钥
S902:编排IPSec隧道
S903a:创建VRF
S903b:创建隧道
S903c:创建接口IP
S903d:配置IKE加密
S903e:配置BGP
S904a:创建隧道
S904b:创建接口IP
S904c:配置IKE加密

图 9

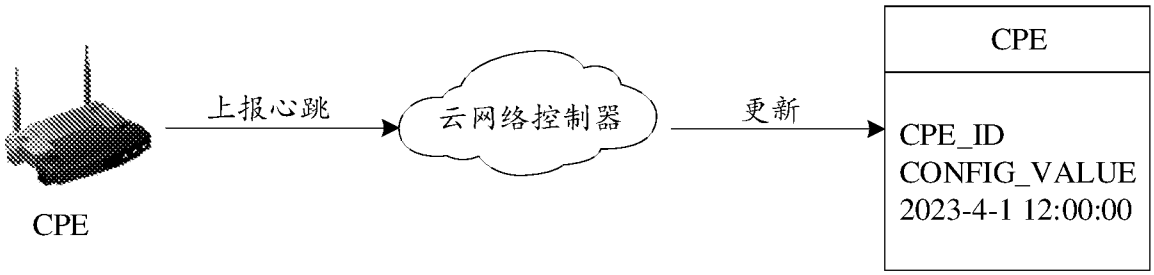

CPE
上报心跳
云网络控制器
更新
CPE
CPE_ID
CONFIG_VALUE
2023-4-1 12:00:00

图 10

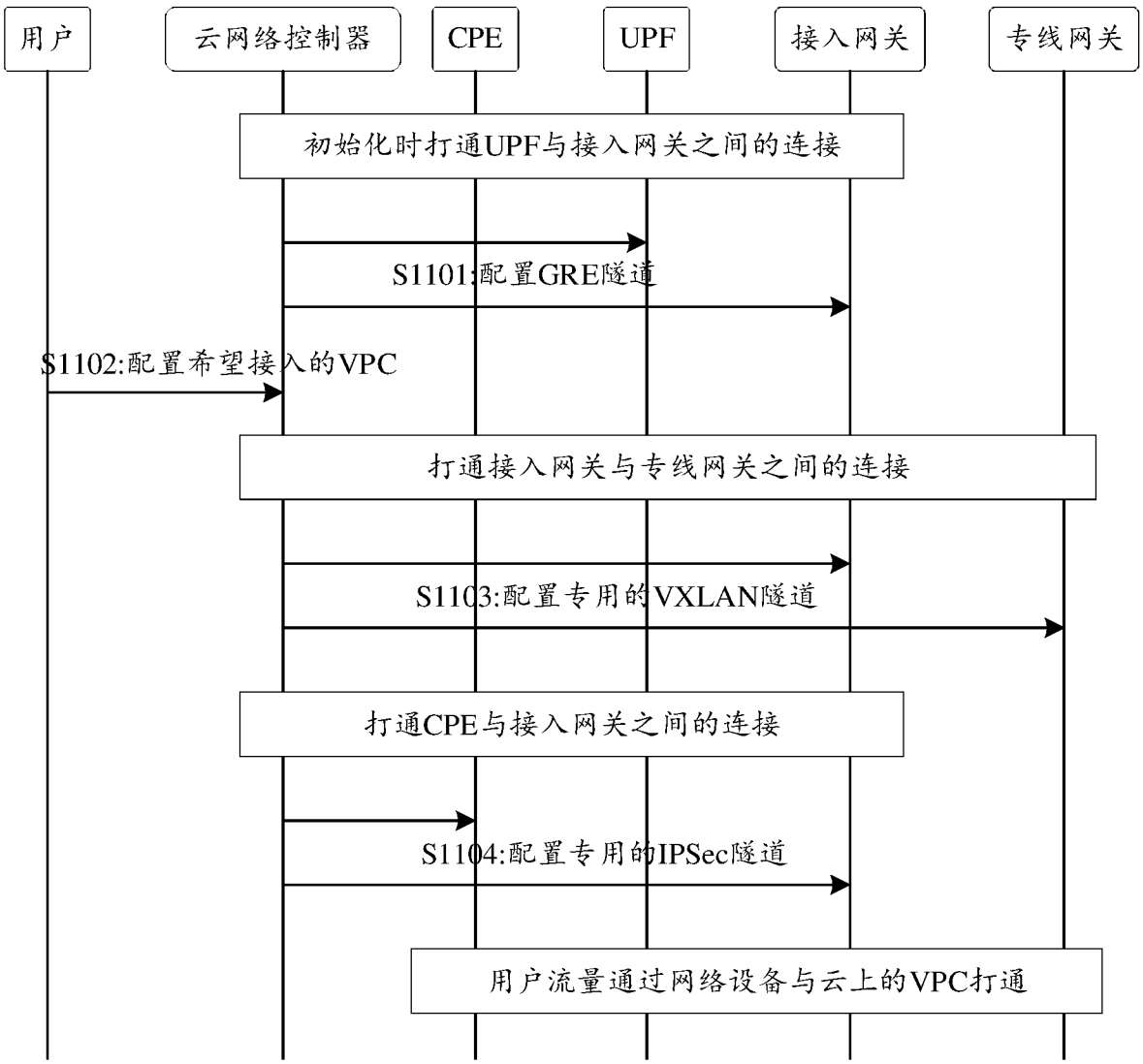

用户
云网络控制器
CPE
UPF
接入网关
专线网关
初始化时打通UPF与接入网关之间的连接
S1101:配置GRE隧道
S1102:配置希望接入的VPC
打通接入网关与专线网关之间的连接
S1103:配置专用的VXLAN隧道
打通CPE与接入网关之间的连接
S1104:配置专用的IPSec隧道
用户流量通过网络设备与云上的VPC打通

图 11

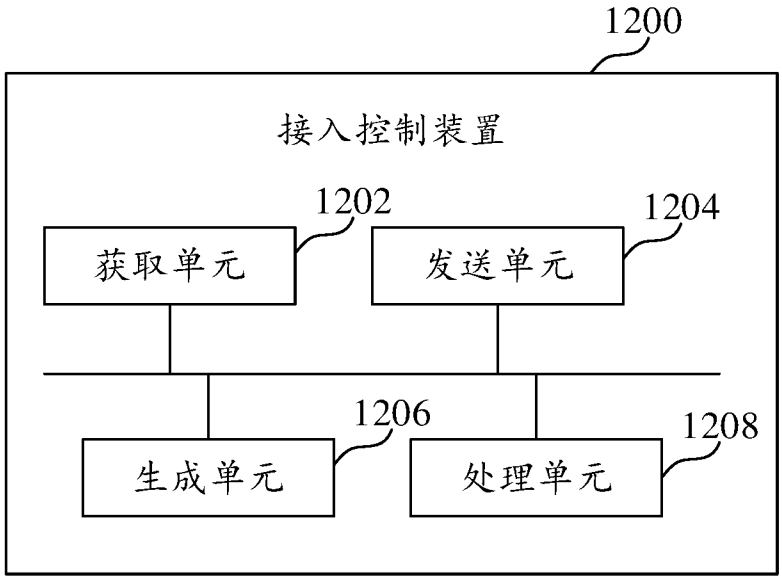

1200
接入控制装置
1202
获取单元
1204
发送单元
1206
生成单元
1208
处理单元

图 12

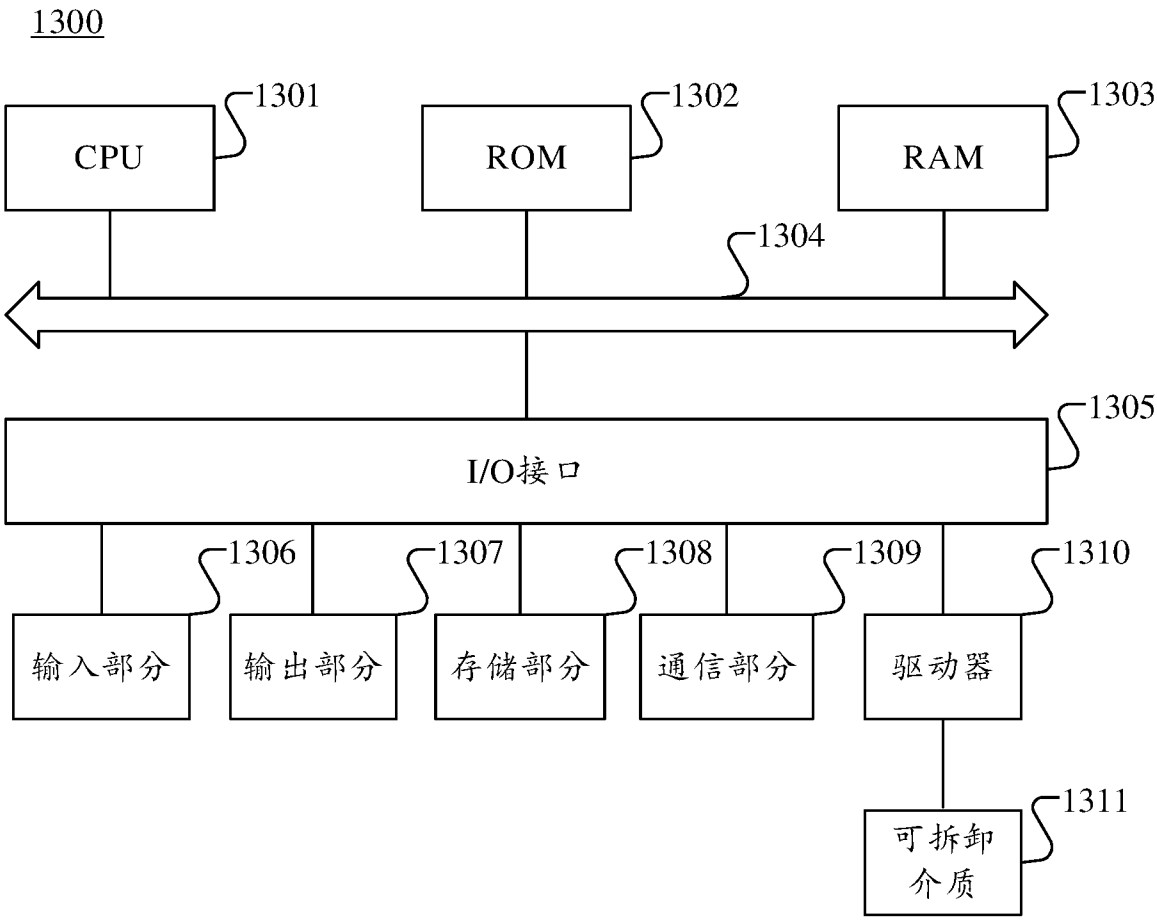

1300
1301
CPU
1302
ROM
1303
RAM
1304
1305
I/O接口
1306
输入部分
1307
输出部分
1308
存储部分
1309
通信部分
1310
驱动器
1311
可拆卸介质

图 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2024/100535

A. CLASSIFICATION OF SUBJECT MATTER

H04W 48/08(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04W48/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNTXT, WPABSC, ENTXTC, CNKI: 接入, 控制, 专用, 专有, 专线, 网关, 隧道, 建立, 配置, 终端, 设备, 用户驻地设备, 上线, 连网; WPABS, VEN, USTXT, EPTXT, WOTXT, 3GPP, IEEE: access, control, controller, private wire, private network, private line, dedicated line, gateway, tunnel, establish, build, configuration, terminal, equipment, device, CPE, customer premises equipment, online

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 106789527 A (CHINA UNITED NETWORK COMMUNICATIONS GROUP CO., LTD.) 31 May 2017 (2017-05-31) claim 1, and description, paragraph 31	1-16
Y	CN 109327375 A (CHINA TELECOM CORP., LTD.) 12 February 2019 (2019-02-12) claims 1-13, and description, paragraphs 45 and 100	1-16
A	CN 109151916 A (BAICELLS TECHNOLOGIES CO., LTD.) 04 January 2019 (2019-01-04) entire document	1-16
A	CN 112995007 A (CHINA MOBILE COMMUNICATIONS CORPORATION, SHAANXI CO., LTD. et al.) 18 June 2021 (2021-06-18) entire document	1-16
A	CN 114844935 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.) 02 August 2022 (2022-08-02) entire document	1-16

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 August 2024	**28 August 2024**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2024/100535

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 9300487 B1 (ANPAT Sourabh et al.) 29 March 2016 (2016-03-29) entire document	1-16

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/100535

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 106789527 A	31 May 2017	CN 106789527 B	03 March 2020
CN 109327375 A	12 February 2019	CN 109327375 B	30 April 2021
CN 109151916 A	04 January 2019	CN 109151916 B	20 June 2023
CN 112995007 A	18 June 2021	CN 112995007 B	15 April 2022
CN 114844935 A	02 August 2022	CN 114844935 B	14 June 2024
		HK 40074014 A0	30 December 2022
US 9300487 B1	29 March 2016	US 2016164806 A1	09 June 2016
		US 9602440 B2	21 March 2017

国际检索报告

国际申请号
PCT/CN2024/100535

A. 主题的分类

H04W 48/08(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC：H04W48/−

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS，CNTXT，WPABSC，ENTXTC，CNKI：接入，控制，专用，专有，专线，网关，隧道，建立，配置，终端，设备，用户驻地设备，上线，连网；WPABS，VEN，USTXT，EPTXT，WOTXT，3GPP，IEEE：access，control，controller，private wire，private network，private line，dedicated line，gateway，tunnel，establish，build，configuration，terminal，equipment，device，CPE，customer premises equipment，online

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 106789527 A (中国联合网络通信集团有限公司) 2017年5月31日 (2017 - 05 - 31) 权利要求1，说明书31段	1−16
Y	CN 109327375 A (中国电信股份有限公司) 2019年2月12日 (2019 - 02 - 12) 权利要求1−13，说明书45,100段	1−16
A	CN 109151916 A (北京佰才邦技术有限公司) 2019年1月4日 (2019 - 01 - 04) 全文	1−16
A	CN 112995007 A (中国移动通信集团陕西有限公司等) 2021年6月18日 (2021 - 06 - 18) 全文	1−16
A	CN 114844935 A (腾讯科技（深圳）有限公司) 2022年8月2日 (2022 - 08 - 02) 全文	1−16
A	US 9300487 B1 (ANPAT Sourabh et al.) 2016年3月29日 (2016 - 03 - 29) 全文	1−16

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“D” 申请人在国际申请中引证的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2024年8月26日	2024年8月28日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 刘磊 电话号码 (+86) 028−62967267

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/100535

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	106789527	A	2017年5月31日	CN	106789527	B	2020年3月3日
CN	109327375	A	2019年2月12日	CN	109327375	B	2021年4月30日
CN	109151916	A	2019年1月4日	CN	109151916	B	2023年6月20日
CN	112995007	A	2021年6月18日	CN	112995007	B	2022年4月15日
CN	114844935	A	2022年8月2日	CN	114844935	B	2024年6月14日
				HK	40074014	A0	2022年12月30日
US	9300487	B1	2016年3月29日	US	2016164806	A1	2016年6月9日
				US	9602440	B2	2017年3月21日