(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
2022 年 12 月 29 日 (29.12.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/268166 A1

(51) 国际专利分类号:
H04W 28/08 (2009.01)

(21) 国际申请号: PCT/CN2022/100809

(22) 国际申请日: 2022 年 6 月 23 日 (23.06.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110703927.1 2021年6月24日 (24.06.2021) CN

(71) 申请人: 中移（成都）信息通信科技有限公司 (CHINA MOBILE (CHENGDU) INFORMATION&TELECOMMUNICATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国四川省成都市中国（四川）自由贸易试验区成都高新区和乐二街150号1号楼2单元, Sichuan 610041 (CN)。 中国移动通信集团有限公司 (CHINA MOBILE COMMUNICATIONS GROUP CO., LTD.) [CN/CN]; 中国北京市西城区金融大街29号, Beijing 100032 (CN)。

(72) 发明人: 唐小勇(TANG, Xiaoyong); 中国四川省成都市中国（四川）自由贸易试验区成都高新区和乐二街150号1号楼2单元, Sichuan 610041 (CN)。 尚宇翔(SHANG, Yuxiang); 中国四川省成都市中国（四川）自由贸易试验区成都高新区和乐二街150号1号楼2单元, Sichuan 610041 (CN)。 韩延涛(HAN, Yantao); 中国四川省成都市中国（四川）自由贸易试验区成都高新区和乐二街150号1号楼2单元, Sichuan 610041 (CN)。 朱磊(ZHU, Lei); 中国四川省成都市中国（四川）自由贸易试验区成都高新区和乐二街150号1号楼2单元, Sichuan 610041 (CN)。 罗柯(LUO, Ke); 中国四川省成都市中国（四川）自由贸易试验区成都高新区和乐二街150号1号楼2单元, Sichuan 610041 (CN)。 游正朋(YOU, Zhengpeng); 中国四川省成都市中国（四川）自由贸易试验区成都高新区和乐二街150号1号楼2单元, Sichuan 610041 (CN)。

(74) 代理人: 北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY

(54) **Title:** COMMUNICATION SYSTEM, METHOD AND APPARATUS, AND FIRST DEVICE AND STORAGE MEDIUM

(54) **发明名称**: 通信系统、方法、装置、第一设备及存储介质

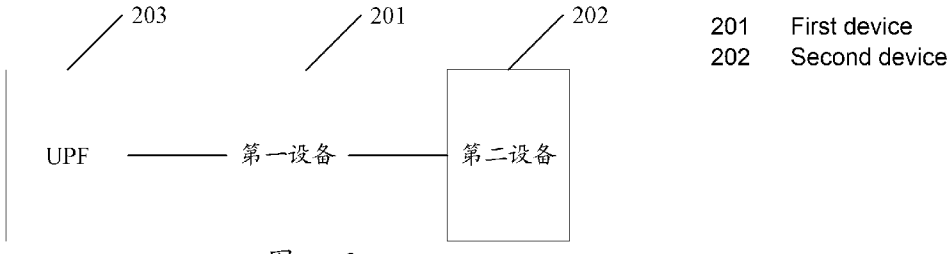

图 2

(57) **Abstract:** Disclosed in the present application are a communication system, method and apparatus, and a first device and a storage medium. The communication system comprises: at least one first device, at least one second device and at least one user plane function (UPF), wherein each first device is connected to at least one second device, each first device is connected to at least one UPF, and the first device is configured to allocate a corresponding second device for service traffic, which is sent by the UPF, of an edge network, so as to shunt the service traffic of the edge network to the corresponding second device, and provide a secure access control function for an application provided by the second device.

(57) **摘要**: 本申请公开了一种通信系统、方法、装置、第一设备及存储介质。其中，通信系统包括：至少一个第一设备、至少一个第二设备、至少一个用户面功能(UPF)；每个第一设备连接至少一个第二设备；每个第一设备连接至少一个UPF；所述第一设备，配置为为UPF发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。

WO 2022/268166 A1

[见续页]

OFFICE)；中国北京市海淀区海淀南路21号中关村知识产权大厦B座2层, Beijing 100080 (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, 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, ME, MG, MK, MN, 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。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, 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))。

通信系统、方法、装置、第一设备及存储介质

相关申请的交叉引用

本申请基于申请号为202110703927.1、申请日为2021年06月24日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本申请涉及通信领域，尤其涉及一种通信系统、方法、装置、第一设备及存储介质。

背景技术

第五代移动通信技术（5G）作为新一代通信技术，具有大带宽、低时延、高可靠、高连接、泛在网等诸多优势，从而推动垂直行业的快速发展与更迭，比如智慧医疗、智慧教育、智慧农业等方向的崛起。

多接入边缘计算（MEC）技术作为5G演进的关键技术之一，是具备无线网络信息应用程序接口（API）交互能力，以及计算、存储、分析功能的信息技术（IT）通用平台；依托MEC技术，可将传统外部应用拉入运营商内部，为用户提供本地化的应用服务，更贴近用户，从而提升用户体验，发挥边缘网络的更多价值。

将5G和MEC技术结合，可以面向不同的行业需求场景，引入不同的技术组合，比如服务质量（QoS）、端到端网络切片、网络能力开放、边缘云等，从而提供定制化的解决方案。

相关技术中，如图1所示，5G与MEC技术结合的方案主要包括:

1）为了使能垂直行业低时延、高带宽、高可靠边缘应用，用户面功能（UPF）下沉到行业客户园区，靠近MEC边缘服务器（也可以称为MEC平台（MEP）），通过UPF的本地分流技术（即上行过滤器/IPv6分支点（UL-CL/IPv6 BP，Uplink Classifier/IPv6 Branching Point））将数据转发到MEP;

2）核心网中的应用功能（AF，Application Function）下沉到MEP侧，为部署于MEP上的应用提供更好的数据流控制策略（比如编码策略、QoS策略、路由策略等）。

然而，上述5G与MEC技术结合的方案存在安全风险。

发明内容

为解决相关技术问题，本申请实施例提供一种通信系统、方法、装置、第一设备及存储介质。

本申请实施例的技术方案是这样实现的：

本申请实施例提供了一种通信系统，包括：至少一个第一设备、至少一个第二设备、至少一个 UPF；其中，

每个第一设备连接至少一个第二设备；每个第一设备连接至少一个 UPF；

所述第一设备，配置为为 UPF 发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。

上述方案中，所述第一设备，还配置为对连接的第二设备进行接入认证。

上述方案中，所述系统还包括：第三设备；其中，

所述第二设备，配置为向所述第一设备发送接入认证信息；接收所述第一设备返回的认证响应信息；

所述第一设备，配置为接收所述第二设备发送的接入认证信息，将所述接入认证信息发送给所述第三设备，接收所述第三设备返回的认证响应信息，以及向所述第二设备返回认证响应信息；

所述第三设备，配置为接收所述第一设备发送的接入认证信息，利用所述接入认证信息对所述第二设备进行接入认证，并向所述第一设备返回认证响应信息。

上述方案中，所述接入认证信息包含所述第二设备的特征。

上述方案中，所述特征包含以下至少之一：

网际互连协议（IP）地址段；

承载的应用；

业务优先级。

上述方案中，所述第一设备，还配置为控制第二设备对网络能力的访问。

上述方案中，

所述第三设备，还配置为向所述第一设备发送第一策略；

所述第一设备，还配置为接收所述第三设备发送的第一策略，基于所述第一策略为第二设备提供的应用提供安全访问控制功能，和/或，基于所述第一策略控制第二设备对网络能力的访问。

上述方案中，所述系统还包括：至少一个第三方网络；其中，

所述第三方网络，配置为为终端提供网络接入；

所述第一设备，还配置为为所述终端选择对应的第二设备，并将对应

第二设备提供的应用通过所述第三方网络提供给所述终端。

上述方案中，所述第一设备，还配置为对第三方网络进行接入认证。

上述方案中，所述系统还包括：第三设备；其中，

所述第三方网络，配置为向所述第一设备发送接入认证信息；并接收所述第一设备返回的认证响应信息；

所述第一设备，配置为接收所述第三方网络发送的接入认证信息，将所述接入认证信息发送给所述第三设备，接收所述第三设备返回的认证响应信息，以及向所述第三方网络返回认证响应信息；

所述第三设备，配置为接收所述第一设备发送的接入认证信息，利用所述接入认证信息对所述第三方网络进行接入认证，并向所述第一设备返回认证响应信息。

上述方案中，所述接入认证信息包含第三方网络的特征。

上述方案中，所述特征包含以下至少之一：

最大带宽；

带宽控制粒度；

IP 地址段；

业务优先级；

承载的应用。

上述方案中，所述第一设备，配置为接入认证通过后，基于安全机制与所述第三方网络进行数据传输。

上述方案中，所述第一设备，还配置为控制所述第三方网络的接入能力。

上述方案中，

所述第三设备，还配置为向所述第一设备发送第二策略；

所述第一设备，还配置为接收所述第三设备发送的第二策略，基于所述第二策略控制所述第三方网络的接入能力。

上述方案中，所述第二策略包含以下之一：

第一接入控制策略；所述第一接入控制策略针对单个第三方网络；

第二接入控制策略；所述第二接入控制策略针对一种类型的第三方网络；

第三接入控制策略；所述第三接入控制策略针对所有第三方网络。

上述方案中，所述第一设备，配置为向所述第三方网络发送第一信息，所述第一信息用于指示所述第三方网络的接入能力；

所述第三方网络，配置为接收所述第一设备发送的第一信息，利用所述第一信息调整自身的接入能力。

上述方案中，所述系统还包括：至少一个第四设备；其中，

所述第四设备，配置为为所述第一设备提供网络能力信息。

上述方案中，所述第一设备，还配置为对第四设备进行接入认证。

上述方案中，所述系统还包括：第三设备；其中，

所述第四设备，还配置为向所述第一设备发送接入认证信息；接收所述第一设备返回的认证响应信息；

所述第一设备，配置为接收所述第四设备发送的接入认证信息，将所述接入认证信息发送给所述第三设备，接收所述第三设备返回的认证响应信息，以及向所述第四设备返回认证响应信息；

所述第三设备，配置为利用所述接入认证信息对所述第四设备进行接入认证，并向所述第一设备返回认证响应信息。

上述方案中，

所述第一设备，还配置为控制所述第四设备的接入能力。

上述方案中，所述第一设备，配置为向所述第四设备发送第二信息，所述第二信息用于指示所述第四设备的接入能力；

所述第四设备，配置为接收所述第一设备发送的第二信息，利用所述第二信息调整自身的接入能力。

上述方案中，

所述第三设备，还配置为向所述第一设备发送第三策略；

所述第一设备，还配置为接收所述第三设备发送的第三策略，并基于所述第三策略控制所述第四设备的接入能力。

上述方案中，所述第一设备，配置为通过至少一个其他第一设备，将终端的业务流进行路由转发，以实现所述终端获取至少一个其他第一设备连接的第二设备提供的应用。

上述方案中，所述系统还包括：第三设备，配置为控制所述至少一个第一设备。

上述方案中，所述第三设备，还配置为对所述至少一个第一设备进行认证。

上述方案中，

所述第一设备，配置为向所述第三设备发送认证信息；并接收所述第三设备返回的认证响应信息；

所述第三设备，配置为接收所述第一设备发送的认证信息，并利用所述认证信息对所述第一设备进行认证，并向所述第一设备返回认证响应信息。

上述方案中，所述第一设备，还配置为监控网络的流量和/或网络状态；并向所述第三设备上报以下信息至少之一：

网络的流量；

计费信息；

网络状态的监控信息；

网络能力的使用信息；

第二设备状态的监控信息。

本申请实施例还提供了一种通信方法，应用于第一设备，包括:

为 UPF 发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。

上述方案中，所述方法还包括:

对连接的第二设备进行接入认证;

和/或，

控制第二设备对网络能力的访问。

上述方案中，所述对连接的第二设备进行接入认证，包括:

接收所述第二设备发送的接入认证信息;

将所述接入认证信息发送给第三设备;

接收到所述第三设备返回的认证响应信息后，向所述第二设备返回认证响应信息。

上述方案中，所述接入认证信息包含所述第二设备的特征。

上述方案中，所述特征包含以下至少之一:

IP 地址段;

承载的应用;

业务优先级。

上述方案中，所述方法还包括:

接收第三设备发送的第一策略;

基于所述第一策略为第二设备提供的应用提供安全访问控制功能，和/或，基于所述第一策略控制第二设备对网络能力的访问。

上述方案中，所述方法还包括:

为接入第三方网络的终端选择对应的第二设备，将对应第二设备提供的应用通过所述第三方网络提供给所述终端。

上述方案中，所述方法还包括:

对所述第三方网络进行接入认证。

上述方案中，所述对所述第三方网络进行接入认证，包括:

接收所述第三方网络发送的接入认证信息;

将所述接入认证信息发送给所述第三设备;

接收到所述第三设备返回的认证响应信息后，向所述第三方网络返回认证响应信息。

上述方案中，所述接入认证信息包含第三方网络的特征。

上述方案中，所述特征包含以下至少之一:

最大带宽;

带宽控制粒度;

IP 地址段;

业务优先级;

承载的应用。

上述方案中，

接入认证通过后，基于安全机制与所述第三方网络进行数据传输。

上述方案中，所述方法还包括：

控制所述第三方网络的接入能力。

上述方案中，所述方法还包括：

接收第三设备发送的第二策略；

基于所述第二策略控制所述第三方网络的接入能力。

上述方案中，所述第二策略包含以下之一：

第一接入控制策略；所述第一接入控制策略针对单个第三方网络；

第二接入控制策略；所述第二接入控制策略针对一种类型的第三方网络；

第三接入控制策略；所述第三接入控制策略针对所有第三方网络。

上述方案中，所述控制所述第三方网络的接入能力，包括：

向所述第三方网络发送第一信息，所述第一信息用于指示所述第三方网络的接入能力。

上述方案中，所述方法还包括：

接收第四设备发送的网络能力信息。

上述方案中，所述方法还包括：

控制所述第四设备的接入能力；

和/或，

对第四设备进行接入认证。

上述方案中，所述控制所述第四设备的接入能力，包括：

向所述第四设备发送第二信息，所述第二信息用于指示所述第四设备的接入能力。

上述方案中，所述方法还包括：

接收所述第三设备发送的第三策略；

基于所述第三策略控制所述第四设备的接入能力。

上述方案中，所述对第四设备进行接入认证，包括：

接收所述第四设备发送的接入认证信息；

将所述接入认证信息发送给第三设备；

接收到所述第三设备返回的认证响应信息后，向所述第四设备返回认证响应信息。

上述方案中，所述方法还包括：

通过至少一个其他第一设备，将终端的业务流进行路由转发，以实现所述终端获取至少一个其他第一设备连接的第二设备提供的应用。

上述方案中，所述方法还包括：

监控网络的流量和/或网络状态；并向第三设备上报以下信息至少之一：

网络的流量;

计费信息;

网络状态的监控信息;

网络能力的使用信息;

第二设备状态的监控信息。

本申请实施例还提供了一种通信装置，设置在第一设备上，包括:

处理单元，配置为为 UPF 发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。

本申请实施例还提供了一种第一设备，包括：处理器及通信接口；其中，

所述处理器，配置为为 UPF 发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。

本申请实施例还提供了一种第一设备，包括：处理器及和配置为存储能够在处理器上运行的计算机程序的存储器，

其中，所述处理器配置为运行所述计算机程序时，执行上述任一方法的步骤。

本申请实施例还提供了一种存储介质，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上述任一方法的步骤。

本申请实施例提供的通信系统、方法、装置、第一设备及存储介质，所述通信系统包括: 至少一个第一设备、至少一个第二设备、至少一个 UPF; 其中，每个第一设备连接至少一个第二设备；每个第一设备连接至少一个 UPF；所述第一设备为 UPF 发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。本申请实施例的方案，通过第一设备，实现 UPF 与第二设备（比如 MEP）之间的网络能力开放的业务代理；如此，能够保障通信系统的数据安全，提高通信系统的网络安全能力，从而提升用户体验。

附图说明

图 1 为相关技术中 5G 与 MEC 技术结合的系统结构示意图;

图 2 为本申请实施例通信系统结构示意图;

图 3 为本申请实施例通信方法的流程示意图;

图 4 为本申请应用实施例 5G 行业云网融合的系统结构示意图;

图 5 为本申请应用实施例 5G 行业云网融合的网络能力开放架构示意图;

图 6 为本申请应用实施例接口形式的 5G 行业云网融合的系统结构示意图;

图 7 为本申请应用实施例实现行业网关对第三方网络的接入认证功能和接入控制功能的流程示意图;

图 8 为本申请应用实施例实现行业网关对第三方网络能力的接入认证功能和接入控制功能的流程示意图;

图 9 为本申请应用实施例实现行业网关对 MEP 的接入认证功能和接入控制功能的流程示意图;

图 10 为本申请应用实施例实现面向 MEP 的网络能力开放功能和自服务网络安全管控功能的流程示意图;

图 11 为本申请实施例通信装置结构示意图;

图 12 为本申请实施例第一设备结构示意图。

具体实施方式

下面结合附图及实施例对本申请再作进一步详细的描述。

相关技术中，图 1 所示的 5G 与 MEC 技术结合的方案具体存在以下安全风险:

第一，UPF 与 MEP 的部署位置导致的安全风险。

具体地，UPF 与 MEP 在功能逻辑上是分开的，但可以通过两种方式部署，分别是：合并部署与分离部署；其中，合并部署是指将 UPF 与 MEP 部署在同一机房甚至同一物理设备上;分离部署是指将 UPF 与 MEP 部署在不同机房。实际应用时，合并部署方式并不适用于垂直行业（比如智慧医疗、智慧教育、智慧农业等），这是因为：如果将 UPF 与 MEP 合并部署在运营商机房，则违背了行业客户对其应用数据不能出园区的安全要求；而如果将 UPF 与 MEP 合并部署在行业客户园区机房,则非常不利于运营商的运维，且会提升针对整个核心网的安全风险。因此，对于垂直行业应用，UPF 与 MEP 应分离部署，具体地，可以将 UPF 部署于运营商机房，并将 MEP 部署于行业客户园区机房。然而，在 UPF 与 MEP 分离部署的场景下，无法保障 UPF 与 MEP 之间的数据安全，存在安全风险。

第二，泛在网络接入导致的安全风险。

具体地，图 1 所示的架构并未涉及非 5G 网络的接入和数据传输，换句话说，相关技术并未给出 5G 与 MEC 技术结合时非 5G 网络的接入方案。而垂直行业的终端的接入技术类型繁多，除 5G 外，还包括第四代移动通信技术（4G）、WiFi、蓝牙（Bluetooth）、紫蜂（Zigbee）、窄带物联网（NB-IoT）、有线网络（Wireline）等，这些非 5G 网络接入的终端数据可能无法通过 5G 网络传输到 MEP,使 MEP 无法对各种接入技术类型的终端数据进行接入控制、流量管控和安全监控，无法保障 MEP 的网络与数据安全，存在安全风

险。

第三，网络能力开放导致的安全风险。

具体地，如图 1 所示，相关技术中，通过 MEP 上的 AF 与 5G 核心网（5GC）的网络开放功能（NEF，Network Exposure Function）对接来实现 MEP 的网络能力开放功能（英文可以表示为 Service Capability Exposure Function，缩写为 SCEF）。然而，由于每个 MEP 上的安全等级不统一，当 MEP 向外开放网络能力时，可能因为某个 MEP 上的网络能力应用存在安全漏洞或是某个 MEP 本身的安全机制问题，导致核心网遭受攻击，存在安全风险。

另外，相关技术中，MEP 只能从 5GC 获取网络能力，而 5GC 所能提供的网络能力不能完全满足及精准覆盖垂直行业的业务需求，比如不能提供非 5G 网络接入的终端的位置信息。同时，MEP 网络能力获取数据源多样，包括 5GC、无线接入网（RAN）以及第三方系统等，但相关技术中缺少对网络能力的统一认证、统一监管和统一结算的方案。

第四，本地分流导致的安全风险。

具体地，如图 1 所示，相关技术中，终端到本地 MEP 的数据转发依赖于 UPF 的 UL-CL/IPv6 BP 技术，该技术基于报文的 IP 五元组或前缀来实现本地分流。实际应用时，对于垂直行业，使用 UL-CL/IPv6 BP 技术进行本地分流，会在公网上暴露行业用户的 MEP 的 IP 地址信息，不仅有用户隐私数据泄露的风险，而且可能会导致针对 MEP IP 地址的网络攻击，存在网络安全风险。

其中，实际应用时，为了避免使用 UL-CL/IPv6 BP 技术进行本地分流导致的网络安全风险，还可以考虑采用为 MEP 设置专用数据网络名称（DNN，Data Network Name）的方式来实现本地分流。然而，这种方式需要为每个 MEP 都配置一个单独的 DNN，需要在核心网进行大量的 DNN 配置。并且，针对一个终端访问多个 MEP 的场景，用户需要在终端上不断的切换 DNN，严重影响用户体验。

另外，实际应用时，在垂直行业应用场景中，除本地分流的需求外，还存在 MEP 之间广域互联的需求，比如不同医院之间的数据共享、远程协同诊断等场景。然而，相关技术中，UPF 只支持终端到数据网络（DN，Data Network）的协议数据单元（PDU，Protocol Data Unit）会话，不支持 DN 到 DN 的连接。换句话说，UPF 只支持终端到 MEP 的数据连接，不支持 MEP 之间的互联。

基于此，在本申请的各种实施例中，设置第一设备（可以称为网关），通过第一设备，实现 UPF 与第二设备（比如 MEP）之间的网络能力开放的业务代理；如此，能够保障通信系统的数据安全，提高通信系统的网络安全能力，从而提升用户体验。

本申请实施例提供一种通信系统，如图 2 所示，该系统包括：至少一

个第一设备 201、至少一个第二设备 202、至少一个 UPF 203；其中，

每个第一设备 201 连接至少一个第二设备 202；每个第一设备 201 连接至少一个 UPF 203；

所述第一设备 201，配置为为 UPF 203 发送的边缘网络的业务流量分配对应的第二设备 202，以将边缘网络的业务流量分流至对应的第二设备 202，并为第二设备 202 提供的应用提供安全访问控制功能。

其中，实际应用时，所述第一设备 201 设置在 UPF 203 与第二设备 202 之间，所述第一设备 201 可以称为网关，也可以称为行业网关，本申请实施例对所述第一设备 201 的名称不作限定，只要能实现所述第一设备 201 的功能即可。

所述第二设备 202 可以是 MEC 网络中的设备，比如 MEP，也就是说，所述第二设备 202 可以称为 MEP，也可以称为 MEC 服务器，本申请实施例对所述第二设备 202 的名称不作限定，只要能实现所述第二设备 202 的功能即可。

实际应用时，所述第二设备 202 提供的应用可以理解为应用服务或应用程序。

实际应用时，针对同一 DNN 内包含多个 MEP 的本地分流，由第一设备 201 为 UPF 203 发送的边缘网络的业务流量分配对应的第二设备 202，与上述的依赖 UPF 的 UL-CL/IPv6 BP 技术相比，能够避免使用 UL-CL/IPv6 BP 技术进行本地分流导致的第二设备 202 的 IP 地址信息在公网上的暴露，从而提高通信系统的网络安全能力；另一方面，与采用为 MEP 设置专用 DNN 的方案相比，无需在核心网进行大量的 DNN 配置；并且，针对一个终端访问多个 MEP 的场景，也无需用户在终端上不断的切换 DNN，从而能够提升用户体验。

实际应用时，所述第一设备 201 需要对所述第二设备 202 进行接入认证，以确定所述第二设备 202 的身份。

基于此，在一实施例中，所述第一设备 201，还可以配置为：

对连接的第二设备 202 进行接入认证。

实际应用时，可以由所述第二设备 202 主动或被动地触发接入认证流程，所述接入认证流程可以利用远程用户拨号认证服务（RADIUS，Remote Authentication Dial In User Service）实现。

实际应用时，所述第二设备 202 可以通过所述第一设备 201 与运营商的管理系统进行交互，以实现接入认证。

基于此，在一实施例中，所述系统还可以包括：第三设备；其中，

所述第二设备 202，可以配置为向所述第一设备 201 发送接入认证信息；接收所述第一设备 201 返回的认证响应信息；

所述第一设备 201，可以配置为接收所述第二设备 202 发送的接入认证信息，将所述接入认证信息发送给所述第三设备，接收所述第三设备返回

的认证响应信息，以及向所述第二设备202返回认证响应信息；

相应地，所述第三设备，可以配置为接收所述第一设备 201 发送的接入认证信息，利用所述接入认证信息对所述第二设备 202 进行接入认证，并向所述第一设备返回认证响应信息。

这里，所述第三设备可以称为运营商的管理系统，比如具体可以是业务支撑系统（BSS，Business Support System）或运营支撑系统（OSS，Operation Support System）。本申请实施例对所述第三设备的名称不作限定，只要实现所述第三设备的功能即可。

在一实施例中，所述接入认证信息可以包含所述第二设备202的特征。其中，所述特征可以包含以下至少之一：

IP 地址段（即 IP 地址范围）；

承载的应用；

业务优先级。

实际应用时，每个第一设备201可能连接多个第二设备202，所述多个第二设备 202 可以通过对应的第一设备 201 进行网络数据的接收与发送；相应地，所述第一设备 201 可以根据连接的多个第二设备 202 中每个第二设备 202 的业务优先级，对所述多个第二设备 202 进行资源调度，比如，为业务优先级高的第二设备 202 提供更高的带宽，再比如，在网络拥塞时优先转发源设备或目的设备为业务优先级高第二设备202的数据。

实际应用时，第二设备 202 的业务优先级可以利用字段“高”、“中”或“低”来表示；或者，所述业务优先级也可以用数字表示，数字越大，业务优先级越高。

实际应用时，第二设备 202 的接入认证信息还可以包含第二设备 202 对应的用户名（即具有第二设备202注册权限的用户名）、用户名对应的密钥等内容。第二设备 202 的认证响应信息可以包含认证结果；在所述认证结果表征认证成功的情况下，所述认证响应信息还可以包含相应第二设备202的身份标识；在所述认证结果表征认证失败的情况下，所述认证响应信息还可以包含认证失败原因。

在一实施例中，所述第一设备201，还配置为控制第二设备202对网络能力的访问。

实际应用时，所述第一设备 201 可以基于本地预设的策略为第二设备 202 提供的应用提供安全访问控制功能，和/或基于本地预设的策略控制第二设备 202 对网络能力的访问；或者，所述第一设备 201 也可以从所述第三设备获取用于为第二设备 202 提供的应用提供安全访问控制功能和/或控制第二设备202对网络能力的访问的策略。

基于此，在一实施例中，所述第三设备，还可以配置为向所述第一设备201发送第一策略；

相应地，所述第一设备201，还可以配置为接收所述第三设备发送的第

一策略，基于所述第一策略为第二设备 202 提供的应用提供安全访问控制功能，和/或，基于所述第一策略控制第二设备 202 对网络能力的访问。

实际应用时，为了满足垂直行业的业务需求，所述通信系统还可以包括第三方网络；所述第一设备 201 还可以实现第三方网络与第二设备 202 之间的网络能力开放的业务代理。

基于此，在一实施例中，所述系统还可以包括：至少一个第三方网络；其中，

所述第三方网络，可以配置为为终端提供网络接入；

所述第一设备 201，还可以配置为为所述终端选择对应的第二设备 202，并将对应第二设备 202 提供的应用通过所述第三方网络提供给所述终端。

实际应用时，所述第三方网络可以理解为非 5G 网络，比如 4G、WiFi、Bluetooth、Zigbee、NB-IoT、Wireline 等。

实际应用时，所述终端可以称为用户设备（UE，User Equipment），也可以称为用户。

实际应用时，所述第一设备 201 具体可以基于所述第一策略为第二设备 202 提供的应用提供核心网和所述第三方网络的安全访问控制功能，和/或，基于所述第一策略控制第二设备 202 对所述核心网和所述第三方网络的网络能力的访问。

实际应用时，所述第一策略可以包含所述第一设备 201 的身份标识、对应的第二设备 202 的身份标识、第一设备 201 与第二设备 202 之间的传输通道的加密策略、对应的第二设备 202 允许访问的网络能力类型列表、对应的第二设备 202 允许访问的网络能力 API 列表、对应的第二设备 202 对网络能力 API 的最大调用次数、对应的第二设备 202 允许访问的自服务网络安全管控 API 列表、对应的第二设备 202 连接第一设备 201 的开启或关闭指示、第一设备 201 与第二设备 202 之间的传输通道的最大带宽、第一设备 201 与第二设备 202 之间的传输通道的最大流量等信息。

实际应用时，所述加密策略可以包括：采用互联网协议安全（IPSec，Internet Protocol Security）协议实现远程接入的虚拟专用网络（VPN，Virtual Private Network）技术。具体地，所述第一设备 201 可以通过第一隧道与所述第二设备 202 进行数据传输，所述第一隧道可以是采用 IPSec 协议实现远程接入的 VPN 技术实现的加密隧道。

实际应用时，所述第一设备 201 基于所述第一策略控制第二设备 202 对网络能力的访问时，具体可以基于所述第一策略，向对应的所述第二设备 202 发送第三信息，所述第三信息用于指示相应第二设备 202 对网络能力的访问；相应地，所述第二设备 202，可以配置为接收所述第一设备 201 发送的第三信息，利用所述第三信息调整自身对网络能力的访问。

实际应用时，所述第三信息可以包含相应第二设备 202 的身份标识、相应第二设备 202 允许访问的网络能力 API 列表、相应第二设备 202 允许

访问的自服务网络安全管控 API 列表、相应第二设备 202 连接第一设备 201 的开启或关闭指示等内容。可以理解，所述第二设备 202 接收到所述第三信息后，可以根据所述第三信息包含的连接第一设备 201 的开启或关闭指示，开启或关闭与对应的第一设备 201 的连接。

实际应用时，所述网络能力 API 列表和所述自服务网络安全管控 API 列表中的 API 是开放的 API（Open API），所述第一设备 201 可以通过这些 Open API 与连接的至少一个第二设备 202 进行交互，在为各第二设备 202 中的不同用户类别提供资源域权限控制与安全访问功能（即为第二设备 202 提供的应用提供安全访问功能）的同时，实现用户对网络、计算等资源的自服务管理等层面的操作。

具体地，所述第二设备 202 可以通过 Open API 操作连接的第一设备 201 的自服务管理功能，比如网络分区权限管理、网络性能要求、业务路由策略、网络切片模板、定位区域大小及位置、接入用户标识等方面的功能。这里，所述第二设备 202 可以向所述第一设备 201 发送对应的管理功能信息，来实现自服务管理功能。其中，网络分区权限管理是指为不同的第二设备 202 选择不同的网络接入方式（比如 4G、5G、WiFi、Bluetooth、Zigbee、NB-IoT、Wireline 等），比如，优先级高的第二设备 202 只允许 Wireline 的网络接入方式，优先级低的第二设备 202 可以允许 WiFi、Bluetooth 等网络接入方式。实际应用时，网络性能要求可以理解为第二设备 202 对带宽的要求；网络切片模板的功能是指对网络切片模板的代理；定位区域大小及位置的功能用于供第二设备 202 确定允许接入哪些区域内的终端；所述接入用户标识可以包括手机号码、用户名或应用身份标识（ID）。

实际应用时，所述第二设备 202 可以通过所述网络能力 API 列表中的网络能力 API，从连接的第一设备 201 获取网络能力开放数据，获取的网络能力开放数据符合相应网络能力 API 的定义；所述网络能力开放数据可以包括：定位能力标签（比如 5G、WiFi、Bluetooth 或全球定位系统（GPS）等）、定位数据、接入用户信息、第三方网络接入列表、网络切片能力数据、QoS 能力数据等。

实际应用时，所述第二设备 202 还可以通过所述自服务网络安全管控 API 列表中的自服务网络安全管控 API，从连接的第一设备 201 获取网络能力开放数据，并基于网络能力开放数据向连接的第一设备 201 发送第一指令；所述第一指令用于指示自服务网络安全管控，即所述第一指令指示对应的管理功能信息；所述第一指令符合相应自服务网络安全管控 API 的定义，所述第一指令可以包含网络分区权限管理、网络性能要求、业务路由策略、网络切片模板配置、定位区域大小及位置配置、接入用户 ID 配置（比如手机号码、用户名或者应用 ID）等内容。

实际应用时，所述第一设备 201 可以通过自身的第一接口，与连接的第二设备 202 进行数据传输；比如，所述第一设备 201 可以通过所述第一

接口接收所述第二设备 202 发送的接入认证信息，并通过所述第一接口向所述第二设备 202 返回认证响应信息；再比如，所述第一接口可以承载所述第二设备 202 为用户提供的服务。

实际应用时，所述第一设备 201 需要对所述第三方网络进行接入认证。

基于此，在一实施例中，所述第一设备 201，还可以配置为对第三方网络进行接入认证。

实际应用时，所述第三方网络可以通过所述第一设备 201 与运营商的管理系统进行交互，以实现接入认证。

基于此，在一实施例中，所述第三方网络，可以配置为向所述第一设备 201 发送接入认证信息；并接收所述第一设备 201 返回的认证响应信息；

所述第一设备 201，可以配置为接收所述第三方网络发送的接入认证信息，将所述接入认证信息发送给所述第三设备，接收所述第三设备返回的认证响应信息，以及向所述第三方网络返回认证响应信息；

相应地，所述第三设备，可以配置为接收所述第一设备 201 发送的接入认证信息，利用所述接入认证信息对所述第三方网络进行接入认证，并向所述第一设备 201 返回认证响应信息。

这里，在一实施例中，所述接入认证信息可以包含第三方网络的特征。

其中，所述特征可以包含以下至少之一：

最大带宽；

带宽控制粒度；

IP 地址段；

业务优先级；

承载的应用。

实际应用时，每个第一设备 201 可以连接多个第三方网络，所述多个第三方网络可以通过相应的第一设备 201 与对应的第二设备 202 进行网络数据的接收和发送；相应地，所述第一设备 201 可以根据连接的多个第三方网络中每个第三方网络的业务优先级，对所述多个第三方网络进行资源调度，比如，为业务优先级高的第三方网络提供更高的带宽，再比如，在网络拥塞时优先转发业务优先级高的第三方网络的数据。

实际应用时，第三方网络的业务优先级可以利用字段“高”、“中”或“低”来表示；或者，所述业务优先级也可以用数字表示，数字越大，业务优先级越高。

实际应用时，第三方网络的接入认证信息还可以包含第三方网络对应的用户名（即具有第三方网络注册权限的用户名）、用户名对应的密钥、用于表征网络类型（比如 4G、WiFi、Bluetooth、Zigbee、NB-IoT、Wireline 等）的网络标识等内容。第三方网络的认证响应信息可以包含认证结果；在所述认证结果表征认证成功的情况下，所述认证响应信息还可以包含相应第三方网络对应的身份标识；在所述认证结果表征认证失败的情况下，

所述认证响应信息还可以包含认证失败原因。

这里，第三方网络的接入认证通过后，所述第一设备 201 可以基于安全机制与所述第三方网络进行数据传输。

基于此，在一实施例中，所述第一设备 201，可以配置为接入认证通过后，基于安全机制与所述第三方网络进行数据传输。

实际应用时，第三方网络的接入认证通过后，所述第一设备 201 还可以基于连接的各个第三方网络的网络标识，实现对不同网络的接入管理、控制、运营与运维等功能。

基于此，在一实施例中，所述第一设备 201，还可以配置为控制所述第三方网络的接入能力。

实际应用时，所述第一设备 201 可以基于本地预设的策略控制所述第三方网络的接入能力；或者，所述第一设备 201 也可以从所述第三设备获取用于控制所述第三方网络的接入能力的策略。

基于此，在一实施例中，所述第三设备，还可以配置为向所述第一设备 201 发送第二策略；

所述第一设备 201，还可以配置为接收所述第三设备发送的第二策略，基于所述第二策略控制所述第三方网络的接入能力。

其中，所述第二策略可以包含以下之一：

第一接入控制策略；所述第一接入控制策略针对单个第三方网络；

第二接入控制策略；所述第二接入控制策略针对一种类型的第三方网络；

第三接入控制策略；所述第三接入控制策略针对所有第三方网络。

实际应用时，所述第一设备 201 可以基于所述第一接入控制策略控制相应第三方网络的能力；所述第一接入控制策略可以包含相应第三方网络对应的身份标识、相应第一设备 201 的身份标识、相应第三方网络的最大接入带宽、相应第三方网络的最大网络流量、相应第三方网络的最长接入时长、相应第三方网络的最大接入用户数、相应第三方网络的计费策略、以及相应第三方网络接入的开启或关闭指示等信息。

实际应用时，所述第一设备 201 可以基于所述第二接入控制策略控制相应类型的第三方网络的能力；所述第二接入控制策略可以包含相应类型的第三方网络的网络标识、相应第一设备 201 的身份标识、相应类型的第三方网络的最大接入带宽、相应类型的第三方网络的最大网络流量、相应类型的第三方网络的最长接入时长、相应类型的第三方网络的最大接入用户数、相应类型的第三方网络的计费策略、以及相应类型的第三方网络接入的开启或关闭指示等信息。

实际应用时，所述第一设备 201 可以基于所述第三接入控制策略控制所有第三方网络的能力；所述第三接入控制策略可以包含相应第一设备 201 的身份标识、相应第一设备 201 连接的所有第三方网络的最大接入带宽、

相应第一设备 201 连接的所有第三方网络的最大网络流量、相应第一设备 201 连接的所有第三方网络的最长接入时长、相应第一设备 201 连接的所有第三方网络的最大接入用户数、相应第一设备 201 连接的所有第三方网络的计费策略、以及相应第一设备 201 连接的所有第三方网络接入的开启或关闭指示等信息。

其中，所述第三方网络的计费策略，可以包含以下至少之一：

基于第三方网络的宽带（即最大带宽值）计费；比如按带宽包年包月计费、按带宽使用时长计费等计费模式；

基于第三方网络的流量（即第三方网络实际传输的数据总量）计费；

基于第三方网络的网络切片的类型和数量计费；

基于第三方网络的 QoS 计费；所述第三方网络的 QoS 可以包含数据传输的速率、时延、抖动、可靠性等；

基于第三方网络接入的用户数计费；比如按最大接入用户数包月包年计费、按实际接入用户数计费等计费模式。

实际应用时，所述第一设备 201 需要指示所述第三方网络的接入能力，以便能够控制第三方网络的接入能力。

基于此，在一实施例中，所述第一设备 201，可以配置为向所述第三方网络发送第一信息，所述第一信息用于指示所述第三方网络的接入能力；

相应地，所述第三方网络，可以配置为接收所述第一设备 201 发送的第一信息，利用所述第一信息调整自身的接入能力。

实际应用时，所述第一信息可以包含相应第三方网络对应的身份标识以及相应第三方网络接入的开启或关闭指示、第三方网络接入开启时网络能力列表等内容。这里，所述第三方网络接入开启时网络能力列表可以包含带宽、带宽控制粒度、接入用户数等。

实际应用时，所述第一设备 201 可以通过自身的第二接口，与连接的第三方网络进行数据传输；比如，所述第一设备 201 可以通过所述第二接口接收所述第三方网络发送的接入认证信息，并通过所述第二接口向所述第三方网络返回认证响应信息；再比如，所述第一设备 201 可以通过所述第二接口向所述第三方网络发送所述第一信息。

实际应用时，所述第一设备 201 可以通过第二隧道与所述第三方网络进行数据传输，所述第二隧道可以实现对接入网络数据的二次封装以保障数据安全、统一协议解析与适配等功能。

实际应用时，所述第一设备 201 还可以获取各种网络（比如包含 5G 网络和/或第三方网络）的网络信息，以提供给需要的设备，比如发送给 MEC 编排器（MEO，MEC Orchestrator）（也可以称为 MEC 应用编排器（MEAO，MEC Application Orchestrator），使得 MEO 至少可以利用所述至少一个网络的网络信息编排所述第二设备 202 上的应用和可用资源。示例性地，所述第一设备 201 可以从第三方网络的管理设备获得第三方网络的网络信息，

可以从 5G 的管理设备获得 5G 网络的网络信息。

实际应用时，所述第一设备需要获取各种网络（比如包含 5G 网络和/或第三方网络）的网络能力信息。

基于此，在一实施例中，所述系统还包括：至少一个第四设备；其中，

所述第四设备，配置为为所述第一设备 201 提供网络能力信息。

实际应用时，所述第四设备可以称为网络能力平台，针对除 5G 网络外的第三方网络，所述第四设备也可以称为第三方网络能力平台，本申请实施例对所述第四设备的名称不作限定，只要能实现所述第四设备的功能即可。

实际应用时，在需要获取 5G 网络的网络能力的情况下，所述第四设备可以包含核心网的网元，比如 AF 等；在需要获取第三方网络的网络能力的情况下，所述第四设备可以包含第三方网络的管理设备。当然，所述第四设备也可以从核心网的网络设备或网元获取 5G 网络的网络能力信息，和/或，从第三方网络的管理设备获取第三方网络的网络能力信息，并将获取的至少一个网络的网络能力信息发送至所述第一设备 201。

实际应用时，所述第一设备 201 需要对所述第四设备进行接入认证。

基于此，在一实施例中，所述第一设备 201，还可以配置为对第四设备进行接入认证。

实际应用时，所述第四设备可以通过所述第一设备 201 与运营商的管理系统进行交互，以实现接入认证。

基于此，在一实施例中，所述第四设备，还可以配置为向所述第一设备 201 发送接入认证信息；接收所述第一设备 201 返回的认证响应信息；

所述第一设备 201，可以配置为接收所述第四设备发送的接入认证信息，将所述接入认证信息发送给所述第三设备，接收所述第三设备返回的认证响应信息，以及向所述第四设备返回认证响应信息；

相应地，所述第三设备，可以配置为利用所述接入认证信息对所述第四设备进行接入认证，并向所述第一设备 201 返回认证响应信息。

实际应用时，所述第四设备的接入认证信息可以包含所述第四设备对应的用户名（即具有第三方网络能力注册权限的用户名）、用户名对应的密钥、用于表征所述第四设备可提供的网络能力列表的类型（比如 NEF/策略与计费规则功能（PCRF，Policy and Charging Rules Function)/网络能力开放功能、定位能力、通信服务管理功能（CSMF，Communication Service Management Function）、网络切片能力等）的网络能力标识、所述第四设备可提供的网络能力 API 列表等内容。

实际应用时，所述第四设备的认证响应信息可以包含认证结果；在所述认证结果表征认证成功的情况下，所述认证响应信息还可以包含所述第四设备的身份标识；在所述认证结果表征认证失败的情况下，所述认证响应信息还可以包含认证失败原因。

实际应用时，所述第四设备的接入认证通过后，所述第一设备 201 可以控制所述第四设备的接入能力。

基于此，在一实施例中，所述第一设备 201，还可以配置为控制所述第四设备的接入能力。

实际应用时，所述第一设备 201 可以通过向所述第四设备发送指示信息来指示所述第三方网络设备调整自身的接入能力。

基于此，在一实施例中，所述第一设备 201，可以配置为向所述第四设备发送第二信息，所述第二信息用于指示所述第四设备的接入能力；

相应地，所述第四设备，可以配置为接收所述第一设备 201 发送的第二信息，利用所述第二信息调整自身的接入能力。

实际应用时，所述第二信息可以包含所述第四设备的身份标识以及所述第四设备接入的开启或关闭指示。换句话说，所述第二信息可以用于指示开启或关闭所述第四设备与所述第一设备 201 的连接。

实际应用时，所述第一设备 201 可以通过自身的第三接口，与所述第四设备进行数据传输；比如，所述第一设备 201 可以通过所述第三接口接收所述第四设备发送的接入认证信息，并通过所述第三接口向所述第四设备返回认证响应信息；再比如，所述第一设备 201 可以通过所述第三接口向所述第四设备发送所述第二信息。当然，所述第一设备 201 还可以通过所述第三接口，从所述第四设备获取网络能力信息（比如最大带宽、带宽控制粒度、接入用户数等），以实现面向第二设备 202 的网络能力开放。

实际应用时，所述第一设备 201 可以基于本地预设的策略控制所述第四设备的接入能力；或者，所述第一设备 201 也可以从所述第三设备获取用于控制所述第四设备的接入能力的策略。

基于此，在一实施例中，所述第三设备，还可以配置为向所述第一设备发送第三策略；

相应地，所述第一设备 201，还可以配置为接收所述第三设备发送的第三策略，并基于所述第三策略控制所述第四设备的接入能力。

其中，所述第三策略可以包含以下之一：

第四接入控制策略；所述第四接入控制策略针对单个第四设备；

第五接入控制策略；所述第五接入控制策略针对一种类型的第四设备；

第六接入控制策略；所述第六接入控制策略针对所有第四设备。

实际应用时，所述第一设备 201 可以基于所述第四接入控制策略控制相应第四设备的接入能力；所述第四接入控制策略可以包含相应第四设备的身份标识、相应第一设备 201 的身份标识、相应第四设备提供的网络能力 API 的最大调用次数、相应第四设备的最长接入时长、相应第四设备的计费策略、以及相应第四设备接入的开启或关闭指示等信息。

实际应用时，所述第一设备 201 可以基于所述第五接入控制策略控制相应类型的第四设备的接入能力；所述第五控制策略可以包含相应类型的

第四设备的网络能力标识、相应第一设备 201 的身份标识、相应类型的第四设备提供的网络能力 API 的最大调用次数、相应类型的第四设备的最长接入时长、相应类型的第四设备的计费策略、以及相应类型的第四设备接入的开启或关闭指示等信息。

实际应用时，所述第一设备 201 可以基于所述第六接入控制策略控制相应第一设备 201 连接的所有第四设备的接入能力；所述第六接入控制策略可以包含相应第一设备 201 的身份标识、相应第一设备 201 连接的所有第四设备提供的网络能力 API 的最大调用次数、相应第一设备 201 连接的所有第四设备的最长接入时长、相应第一设备 201 连接的所有第四设备的计费策略、以及相应第一设备 201 连接的所有第四设备接入的开启或关闭指示等信息。

其中，所述第四设备的计费策略，可以包含以下至少之一：

基于第四设备提供的网络能力 API 的实际调用次数计费；

基于第四设备的流量（即第四设备提供的网络能力实际传输的数据总量）计费；

基于第四设备可提供的网络能力列表的类型计费；即针对不同的网络能力列表的类型指定不同计费模式及价格；

基于第四设备提供的网络能力的数据来源计费；即针对不同的网络能力的数据来源指定不同计费模式及价格。

实际应用时，在所述通信系统包括至少两个第一设备 201 的情况下，所述至少两个第一设备 201 之间需要建立连接，以使每个第一设备 201 可以通过其他第一设备 201 将终端的业务流进行路由转发。

基于此，在一实施例中，所述第一设备 201，可以配置为通过至少一个其他第一设备 201，将终端的业务流进行路由转发，以实现所述终端获取至少一个其他第一设备 201 连接的第二设备 202 提供的应用。

实际应用时，所述至少两个第一设备 201 可以组成广域传输网络，实现各园区/组织之间的网络互联互通，以承载多个第二设备 202 之间的业务协同。

实际应用时，所述第一设备 201 可以通过自身的第四接口，与至少一个其他第一设备 201 进行数据传输；所述第四接口可以基于软件定义广域网（SD-WAN，Software Defined Wide Area Network）功能实现。

实际应用时，需要对至少一个第一设备 201 进行管理和控制。

基于此，在一实施例中，所述第三设备，还可以配置为控制所述至少一个第一设备 201。

实际应用时，所述第三设备需要对所述第一设备 201 进行认证。

基于此，在一实施例中，所述第三设备，还可以配置为对所述至少一个第一设备 201 进行认证。

具体地，在一实施例中，所述第一设备 201，可以配置为向所述第三设

备发送认证信息；并接收所述第三设备返回的认证响应信息；

相应地，所述第三设备，配置为接收所述第一设备 201 发送的认证信息，并利用所述认证信息对所述第一设备 201 进行认证，并向所述第一设备 201 返回认证响应信息。

实际应用时，所述第一设备 201 的认证信息可以包含所述第一设备 201 对应的用户名（即具有第一设备 201 的注册权限的用户名）、用户名对应的密钥、所述第一设备 201 支持接入的网络类型列表、所述第一设备 201 支持接入的网络能力类型列表、所述第一设备 201 支持的最大带宽容量、所述第一设备 201 支持的带宽控制粒度等内容。

实际应用时，所述第一设备 201 的认证响应信息可以包含认证结果；在所述认证结果表征认证成功的情况下，所述认证响应信息还可以包含所述第一设备 201 的身份标识；在所述认证结果表征认证失败的情况下，所述认证响应信息还可以包含认证失败原因。

实际应用时，为了使所述第三设备实现所述通信系统的计费和运营，所述第一设备 201 需要监控网络的流量和/或网络状态，并将监控到的信息上报给所述第三设备。

基于此，在一实施例中，所述第一设备 201，还可以配置为监控网络的流量和/或网络状态；并向所述第三设备上报以下信息至少之一：

网络的流量；

计费信息；

网络状态的监控信息；

网络能力的使用信息；

第二设备状态的监控信息。

实际应用时，所述网络状态的监控信息可以包含所述第一设备 201 的身份标识、本次网络状态监控对应的统计时间周期、第三方网络状态的统计信息、第四设备状态的统计信息、第二设备 202 状态的统计信息、以及计费明细等内容。

其中，所述第三方网络状态的统计信息，可以理解为所述第一设备 201 连接的所有第三方网络中每个第三方网络的状态的监控统计信息；所述第三方网络状态的统计信息可以包含第三方网络的身份标识、第三方网络的网络标识、第三方网络的吞吐率、第三方网络的流量、第三方网络的接入时长等内容。

所述第四设备状态的统计信息，可以理解为所述第一设备 201 连接的所有第四设备中每个第四设备的状态的监控统计信息；所述第四设备状态的统计信息可以包含第四设备的身份标识、第四设备的网络能力标识、第四设备提供的网络能力 API 的调用次数、第四设备的流量、第四设备的接入时长等内容。

所述第二设备 202 状态的统计信息，可以理解为所述第一设备 201 连

接的所有第二设备 202 中每个第二设备 202 的状态的监控统计信息；所述第二设备 202 状态的统计信息可以包含第二设备 202 的身份标识、第二设备 202 的吞吐率、第二设备 202 的流量、第二设备 202 对网络能力 API 的调用次数、第二设备 202 的接入时长等内容。

实际应用时，所述计费明细，可以根据第三方网络的计费策略及第四设备的计费策略计算生成。

实际应用时，所述第一设备 201 可以通过自身的第五接口，与所述第三设备进行数据传输；比如，所述第一设备 201 可以通过所述第五接口向所述第三设备发送认证信息，并通过所述第五接口接收所述第三设备返回的认证响应信息；再比如，所述第一设备 201 可以通过所述第五接口接收所述第三设备发送的策略（即所述第一策略、所述第二策略和所述第三策略）。当然，所述第一设备 201 还可以通过所述第五接口向所述第三设备上报信息（即网络的流量、计费信息、网络状态的监控信息、网络能力的使用信息、第二设备状态的监控信息等）。

实际应用时，所述系统还可以包括第五设备，配置为编排所述第二设备 202 上的应用和可用资源；相应地，所述第一设备 201 可以从连接的至少一个第三方网络获取每个第三方网络的网络信息，并从核心网的网络设备或网元（比如 AF、UPF 等）获取 5G 网络的网络信息，向所述第五设备发送得到的 5G 网络或第三方网络的网络信息；所述第五设备接收所述第一设备 201 发送的至少一个网络（可以包含 5G 网络和/或第三方网络）的网络信息，至少可以利用所述至少一个网络的网络信息编排所述第二设备 202 上的应用和可用资源。

实际应用时，所述第五设备可以称为 MEO 或 MEAO，本申请实施例对所述第五设备的名称不作限定，只要能实现所述第五设备的功能即可。

实际应用时，所述第一设备 201 可以通过所述第二接口获取第三方网络的网络信息，通过自身的第六接口从核心网的网络设备或网元获取 5G 网络的网络信息，并可以通过自身的第七接口向所述第五设备发送得到的 5G 网络和/或第三方网络的网络信息；所述第五设备接收到至少一个网络的网络信息后，至少可以利用所述至少一个网络的网络信息，对所述第二设备 202 上的应用和可用资源进行合理、有效地编排；所述合理、有效地编排可以理解为：所述第五设备可以基于所述至少一个网络的网络信息，在编排第二设备 202 上的应用和可用资源时实现网络的负载均衡，比如，当 WiFi 网络的运行状态较差时，所述第五设备可以自动将运行在 WiFi 网络中的应用切换到运行良好的 5G 网络中运行。

实际应用时，所述网络信息可以包含网络类型（即网络标识）、网络运行状态、网络资费信息、网络的运营维护信息等内容；所述网络资费信息，可以包含网络的计费规则、网络的计费明细、网络的共享配额策略、网络的终端绑定策略、网络的限速策略、网络的限量策略等内容；所述网络的

运营维护信息可以包含网络的带宽限制信息、网络的带宽利用率、网络的上行和/或下行流量的使用情况、流量余额等内容。

基于上述系统架构，本申请实施例还提供了一种通信方法，应用于第一设备，如图 3 所示，该方法包括:

步骤 301: 为 UPF 发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。

其中，在一实施例中，如图 3 所示，所述方法还可以包括:

步骤 302: 对连接的第二设备进行接入认证。

在一实施例中，所述方法还可以包括:

控制第二设备对网络能力的访问。

在一实施例中，所述对连接的第二设备进行接入认证，可以包括:

接收所述第二设备发送的接入认证信息;

将所述接入认证信息发送给第三设备;

接收到所述第三设备返回的认证响应信息后，向所述第二设备返回认证响应信息。

在一实施例中，所述接入认证信息可以包含所述第二设备的特征。

其中，所述特征可以包含以下至少之一:

IP 地址段;

承载的应用;

业务优先级。

在一实施例中，所述方法还可以包括:

接收第三设备发送的第一策略;

基于所述第一策略为第二设备提供的应用提供安全访问控制功能，和/或，基于所述第一策略控制第二设备对网络能力的访问。

在一实施例中，所述方法还可以包括:

为接入第三方网络的终端选择对应的第二设备，将对应第二设备提供的应用通过所述第三方网络提供给所述终端。

在一实施例中，所述方法还可以包括:

对所述第三方网络进行接入认证。

在一实施例中，所述对所述第三方网络进行接入认证，可以包括:

接收所述第三方网络发送的接入认证信息;

将所述接入认证信息发送给所述第三设备;

接收到所述第三设备返回的认证响应信息后，向所述第三方网络返回认证响应信息。

在一实施例中，所述接入认证信息可以包含第三方网络的特征。

其中，所述特征可以包含以下至少之一:

最大带宽;

带宽控制粒度;

IP 地址段;

业务优先级;

承载的应用。

在一实施例中，接入认证通过后，所述第一设备可以基于安全机制与所述第三方网络进行数据传输。

在一实施例中，所述方法还可以包括:

控制所述第三方网络的接入能力。

在一实施例中，所述方法还可以包括:

接收第三设备发送的第二策略;

基于所述第二策略控制所述第三方网络的接入能力。

其中，所述第二策略可以包含以下之一:

第一接入控制策略；所述第一接入控制策略针对单个第三方网络;

第二接入控制策略；所述第二接入控制策略针对一种类型的第三方网络;

第三接入控制策略；所述第三接入控制策略针对所有第三方网络。

在一实施例中，所述控制所述第三方网络的接入能力，可以包括:

向所述第三方网络发送第一信息，所述第一信息用于指示所述第三方网络的接入能力。

在一实施例中，所述方法还可以包括:

接收第四设备发送的网络能力信息。

在一实施例中，所述方法还可以包括:

控制所述第四设备的接入能力;

和/或，

对第四设备进行接入认证。

在一实施例中，所述控制所述第四设备的接入能力，可以包括:

向所述第四设备发送第二信息，所述第二信息用于指示所述第四设备的接入能力。

在一实施例中，所述方法还可以包括:

接收所述第三设备发送的第三策略;

基于所述第三策略控制所述第四设备的接入能力。

在一实施例中，所述对第四设备进行接入认证，可以包括:

接收所述第四设备发送的接入认证信息;

将所述接入认证信息发送给第三设备;

接收到所述第三设备返回的认证响应信息后，向所述第四设备返回认证响应信息。

在一实施例中，所述方法还可以包括:

通过至少一个其他第一设备，将终端的业务流进行路由转发，以实现

所述终端获取至少一个其他第一设备连接的第二设备提供的应用。

在一实施例中，所述方法还可以包括:

监控网络的流量和/或网络状态; 并向第三设备上报以下信息至少之一:

网络的流量;

计费信息;

网络状态的监控信息;

网络能力的使用信息;

第二设备状态的监控信息。

本申请实施例提供的通信系统和通信方法，第一设备为 UPF 发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。本申请实施例的方案，通过第一设备，实现 UPF 与第二设备（比如 MEP）之间的网络能力开放的业务代理; 如此，能够保障通信系统的数据安全，提高通信系统的网络安全能力，从而提升用户体验。

下面结合应用实施例对本申请再作进一步详细的描述。

在本应用实施例中，第一设备称为行业网关（英文可以表示为 iGW）; 第二设备为 MEP; 第三设备称为 BSS 或 OSS 系统，简称为 BSS/OSS; 第四设备称为第三方网络能力。

在本应用实施例中，如图 4 所示，通过引入行业网关，解决相关技术中 5G 与 MEC 技术结合的方案中存在的技术问题。所述行业网关部署在 UPF 与 MEP 之间，具备以下五个功能中的至少一种功能:

第一，多制式网络接入控制功能。

具体地，通过所述行业网关，可以实现第三代合作伙伴计划（3GPP）移动网络（比如 4G、5G、NB-IoT 等）、非 3GPP（non-3GPP）移动网络（比如 WiFi、Bluetooth、Zigbee 等）以及固定网络（比如 Wireline、光纤、切片分组网（SPN，Slicing Packet Network）、光传送网（OTN，Optical Transport Network）等）等网络的统一接入与管理。

该功能具有以下关键特性:

1）多制式网络接入能力; 即所述行业网关支持 3GPP 移动网络、non-3GPP 移动网络以及固定网络等不同制式的网络的接入能力。

2）多制式网络接入识别与标签功能; 即所述行业网关可以对不同制式的网络进行接入认证，并在完成接入认证后，为不同制式的网络添加网络标签（即上述网络标识），以识别不同制式的网络对应的网络类型（比如 3GPP 移动网络、non-3GPP 移动网络以及固定网络等）。所述行业网关还可以基于所述网络标签，实现对不同制式的网络的接入管理、控制、运营及运维等功能。

3）多制式网络的连接建立与释放功能; 即所述行业网关可以在相关技术中的 IP 协议的基础上，融合网络标签、统一认证、网络能力（比如带宽、

带宽控制粒度、接入用户数等）列表、网络接入状态（开启状态（On）/关闭状态（Off））等信息，建立与不同制式的网络的连接，并具备不同制式的网络连接的释放功能。

第二，网络广域互联功能。

具体地，多个行业网关可以组成广域传输网络，实现各园区/组织之间的网络互联互通，以承载多个 MEP 之间的业务协同。

该功能具有以下关键特性:

1）智能路由功能；即在 SD-WAN、网络功能虚拟化基础设施解决方案（NFVI，Network Function Virtualization Infrastructure）等技术的基础上，增加所述行业网关与 UE 之间的信息交互，交互的信息包括业务路由地址、业务传输 QoS 要求等内容，以实现从 UE 到不同 MEC 边缘云的智能业务访问。其中，所述业务路由地址可以包含 DNN 和目的 MEC 的 IP 地址等内容。

2）MEC 实体功能类似 UE 化；即通过行业网关 MEC 可以通过有线网络与 5GC 的接入及移动性管理功能（AMF，Access and Mobility Management Function）、进程管理功能（SMF，Session Management Function）、PCRF 等网元直接连接，使得 MEC 的功能类似于 UE，从而通过行业网关，实现了将 UE 与固定 MEC 之间的通信、MEC 与 MEC 之间的通信均统一到 5GC 的接入与管理流程中。

第三，多类型网络能力接入与开放功能。

具体地，所述行业网关可以对接 5GC、RAN、第三方网络（即非 5G 网络，比如 4G、WiFi、Bluetooth、Zigbee、NB-IoT、Wireline 等）的网络能力，通过统一的 API（即 Open API）开放给 MEP 使用，并对网络能力使用情况进行统一监控与结算，实现泛在网络能力的接入与开放功能。

该功能具有以下关键特性:

1）多类型网络能力接入；即所述行业网关可以支持 NEF、PCRF、网络能力开放功能（SCEF）、定位能力、CSMF、网络切片等能力的接入。

2）多类型网络能力开放；即所述行业网关可以通过 Open API 向 MEP 开放定位能力、接入用户信息、多制式网络接入列表、网络切片能力、QoS 等能力。

第四，多制式网络流量监控与计费功能。

具体地，所述行业网关可以作为泛在全连接网络的综合接入设备，实时监控不同制式的网络（即不同类型的网络，比如 5G、4G、WiFi、Bluetooth、Zigbee、NB-IoT、Wireline 等）的流量与网络使用情况，实现计费功能并实时上报给 BSS/OSS，从而实现基于不同量纲的计费与运营策略。

该功能具有以下关键特性:

1）多维度流量与网络监控；即所述行业网关可以支持对不同制式的网络的单独流量统计与网络监控，并通过融合了网络标签、流量数据、网络状态的信令上报给 OSS;

2）多维度计费量纲；即所述行业网关可以支持基于不同种类的网络流量、多类型网络能力调用次数或者调度时长、MEP 能力等信息进行计费，并通过融合了计费量纲标签和具体的计费数值的信令上报给 BSS/OSS。

第五，自服务资源管理功能。

具体地，所述行业网关可以通过 Open API 与 MEP 进行交互，在为 MEP 中的不同用户类别提供资源域权限控制与安全访问控制功能的同时，实现用户对网络、计算等资源的自服务管理等层面的操作；即 MEP 可以通过 Open API 操作所述行业网关的网络分区权限管理、网络性能要求（比如带宽）、业务路由策略、网络切片模板（即网络切片模板的代理功能）、定位区域大小及位置、接入用户 ID（比如手机号码、用户名或者应用 ID）等方面的功能。

其中，网络分区权限管理是指不同的 MEP 具有不同的网络接入权限，比如优先级高的 MEP 只允许有线网络接入，优先级低的 MEP 可以允许 WiFi、Bluetooth 等网络接入；定位区域大小及位置是指每个 MEP 可以配置允许哪些区域内的终端接入。

在本应用实施例中，如图 5 所示，所述行业网关实际上充当了 MEP 与 RAN 之间、MEP 与 5GC 之间、以及 MEP 与第三方系统（可以包括第三方网络和第三方网络能力）之间的网络能力开放的代理角色，在所述行业网关通过代理方式进行网络能力开放的基础上，所述行业网关还可以将网络能力经过处理后，以报告的形式间接开放给 MEP。

在本应用实施例中，对所述行业网关与其他功能实体之间的接口进行了全新定义，如图 6 所示，所述行业网关通过接口 I1 至 I5 实现上述功能。

首先，对接口 I1（即上述第二接口）的功能进行详细说明。

接口 I1 是所述行业网关与第三方网络的通信接口，用于实现第三方网络的接入认证功能，并用于承载所述行业网关与所述第三方网络之间的数据传输。

具体地，接口 I1 支持的关键功能包括:

1）第三方网络的接入认证。这里，第三方网络可以主动或被动地触发接入认证流程，以实现第三方网络的安全接入、接入网络的标识区分（即上述网络标签和网络标识）等功能。

2）第三方网络的接入控制。这里，所述行业网关可以控制是否允许第三方网络接入，并可以主动切断与第三方网络的数据传输等功能。

3）第三方网络的数据传输。这里，所述行业网关可以通过专用的隧道（即上述第二隧道）实现与第三方网络的数据传输功能，该隧道实现对接入网络数据的二次封装以保障数据安全、统一协议解析与适配等功能。

其次，对接口 I2（即上述第三接口）的功能进行详细说明。

接口 I2 是所述行业网关与第三方网络能力的通信接口，用于实现第三方网络能力的接入与认证功能，并用于承载所述行业网关与所述第三方网

络能力之间的数据传输，比如从第三方网络能力获取网络能力数据。

具体地，接口 I2 支持的关键功能包括:

1）第三方网络能力的接入认证。这里，第三方网络能力可以主动或被动地触发接入认证流程，以实现第三方网络能力的安全接入、接入的网络能力的标识区分（即上述的网络能力标识，可以表征 NEF/PCRF/CSMF、定位能力、CSMF、网络切片等能力）等功能。

2）第三方网络能力的接入规则与控制。这里，所述行业网关可以通过网络能力接入状态指示（On/ Off）控制是否允许第三方网络能力接入，并可以获取第三方网络能力的网络能力列表（可以包含带宽、带宽控制粒度、接入用户数等信息）。

3）第三方网络能力数据获取。这里，所述行业网关可以根据第三方网络能力提供的网络能力数据获取网络能力 API ，实现第三方网络能力数据的获取功能。

第三，对接口 I3（即上述第五接口）的功能进行详细说明。

接口 I3 是所述行业网关与 BSS/OSS 的通信接口，用于支持策略配置功能与运行状态监控功能。

具体地，接口 I3 支持的关键功能包括:

1）行业网关的接入认证。这里，行业网关可以主动或被动地触发接入认证流程; 行业网关与 BSS/OSS 交互的信息可以包括: 行业网关设备 ID(即上述第一设备 201 的身份标识)、行业网关支持的接入网络能力列表、是否允许行业网关接入等内容。

2）第三方网络的接入控制。这里，BSS/OSS 可以向行业网关下发第三方网络的接入策略; 行业网关与 BSS/OSS 交互的信息可以包括: 网络类型标签（即上述网络标签和网络标识）、网络认证信息、带宽、流量、计费控制、网络接入状态指示（On/ Off）等内容。

3）第三方网络能力的接入控制。这里，BSS/OSS 可以向行业网关下发第三方网络能力的接入策略; 行业网关与 BSS/OSS 交互的信息可以包括: 网络能力类型标签（即上述网络能力标识）、网络能力认证信息、网络接入状态指示（On/ Off）等内容。

4）MEP 的接入控制。这里，行业网关与 BSS/OSS 交互的信息可以包括: MEP 接入加密策略、允许开放的网络能力列表等内容，从而实现行业网关接入 MEP 的功能。

5）网络状态监控功能。这里，行业网关可以实时监控当前的网络状态; 行业网关与 BSS/OSS 交互的信息可以包括: 融合了网络标签、流量数据、网络状态的运维监控信息，以及融合了计费量纲标签和具体计费数值的计费数据信息。

第四，对接口 I4（即上述第一接口）的功能进行详细说明。

接口 I4 是行业网关与 MEP 的通信接口，用于承载行业网关与 MEP 之

间的数据传输，并实现面向 MEP 的网络能力开放以及自服务网络安全管控功能。

具体地，接口 I4 支持的关键功能包括:

1）MEP 的接入认证。这里，MEP 可以主动或被动地触发接入认证流程；所述接入认证流程可以基于 RADIUS 等技术实现。

2）行业网关与 MEP 之间的数据传输。这里，行业网关可以通过 IPSec/VPN（即采用 IPSec 协议实现远程接入的 VPN 技术）加密隧道（即上述第一隧道）等方式实现与 MEP 之间的数据传输功能。

3）面向 MEP 的网络能力开放功能。这里，行业网关与 MEP 交互的信令可以包括定位能力标签（比如 5G、WiFi、Bluetooth、GPS 等）、定位数据、接入用户信息、多制式网络接入列表、网络切片能力、QoS 能力等信息。

4）面向 MEP 的自服务网络安全管控功能。这里，MEP 可以通过 Open API 操作行业网关的网络分区权限管理、网络性能要求、业务路由策略、网络切片模板、定位区域大小及位置、接入用户 ID（手机号码、用户名或者应用 ID）等方面的功能。

第五，对接口 I5（即上述第四接口）的功能进行详细说明。

接口 I5 是行业网关与其他行业网关之间的通信接口，用于实现行业网关之间的广域互联功能。实际应用时，接口 I5 可以基于 SD-WAN 功能实现，也可通过使能边缘计算 MEP 类 UE 化，通过通用无线分组业务（GPRS）隧道传输协议（GTP）用户平面（GTP-U）隧道实现 MEP 与 MEP 之间的通信并统一到 5GC 的接入与管理流程中。

在本应用实施例中，接口 I1 至 I5 在支持上述功能时承载了所述行业网关与其他功能实体之间交互的信息，下面对接口 I1 至 I5 承载的信息进行详细说明。

首先，对接口 I1 承载的信息进行详细说明。

1）基于接口 I1 实现第三方网络的接入认证功能时，第三方网络可以通过接口 I1 向行业网关上报接入认证信息；所述接入认证信息包含的内容如表 1 所示；其中，如表 2 所示，网络类型标识（即上述网络标识）可以通过多种不同的数据类型表示。行业网关完成第三方网络的接入认证后，可以通过接口 I1 向第三方网络返回认证响应信息；所述认证响应信息包含的内容如表 3 所示；其中，如表 4 所示，网络身份标识可以通过多种不同的数据类型表示。

参数名	数据类型	说明
用户名	字符串（String）	具有第三方网络注册权限的用户名
密钥	String	用户名对应的密钥
网络类型标识	如表 2 所示	用于表示第三方网络的网络类型，比如 4G、WiFi、Bluetooth、Zigbee、NB-IoT、

		Wireline 等
最大带宽	编号或整数（Number）	第三方网络所支持的最大带宽
带宽控制粒度	Number	第三方网络所支持的带宽控制粒度
IP 地址段	String	第三方网络的 IP 地址段
业务优先级	String 或 Number	第三方网络的业务优先级
承载的应用	String	第三方网络所承载的应用

表 1

数据类型	说明
String	每一种网络类型用字符串来表示，比如“4G”、“WiFi6”、“Wireline”等
Number	每一种网络类型用编号来表示，比如 01 代表 Wireline，03 代表 WiFi 等
位图（Bitmap）	用每一个 bit 位来标识一种网络类型，比如 bit0 标识 Wireline，bit1 标识 4G，bit2 标识 WiFi 等；bit 位值为 0 表示不包含该 bit 位标识的网络类型；bit 位值为 1 表示包含该 bit 位标识的网络类型

表 2

参数名	数据类型	说明
认证结果	Boolean	认证成功或失败
错误原因	String	如果认证失败，返回错误码及错误原因描述
网络身份标识	如表 4 所示	如果认证成功，返回该第三方网络在通信系统内唯一的身份标识

表 3

数据类型	说明
String	网络身份标识用字符串来表示，比如“CMHW5G001”
ID 编号	网络身份标识用 ID 编号来表示，比如 0102003059，该编号的第 1-2 位表示运营商、第 3-5 位表示设备提供商、第 6-7 位表示网络类型、第 8-10 位为通信系统的内部编号

表 4

2）基于接口 I1 实现第三方网络的接入控制功能时，行业网关可以通过接口 I1 向第三方网络发送网络接入控制信息（即上述第一信息），以实现对第三方网络的接入控制功能；所述网络接入控制信息包含的内容如表 5 所示。

参数名	数据类型	说明
网络身份标识	如表 4 所示	第三方网络在通信系统内唯一的身份标识

网络接入状态指示（On/ Off）	Boolean	第三方网络接入的开启或关闭指示

表 5

3）行业网关还可以通过接口 I1 向第三方网络发送自服务网络安全管控指令（即上述第一指令），以实现面向 MEP 的自服务网络安全管控功能。

其次，对接口 I2 承载的信息进行详细说明。

1）基于接口 I2 实现第三方网络能力的接入认证功能时，第三方网络能力可以通过接口 I1 向行业网关上报接入认证信息；所述接入认证信息包含的内容如表 6 所示；其中，如表 7 所示，网络能力类型标识（即上述网络能力标识）可以通过多种不同的数据类型表示；如表 8 所示，网络能力 API 列表也可以通过多种不同的数据类型表示。行业网关完成第三方网络能力的接入认证后，可以通过接口 I1 向第三方网络能力返回认证响应信息；所述认证响应信息包含的内容如表 9 所示；其中，如表 10 所示，网络能力身份标识可以通过多种不同的数据类型表示。

参数名	数据类型	说明
用户名	String	具有第三方网络能力注册权限的用户名
密钥	String	用户名对应的密钥
网络能力类型标识	如表 7 所示	第三方网络能力可提供的网络能力列表，比如 NEF/PCRF/SCEF、定位能力、CSMF、网络切片等
网络能力 API 列表	如表 8 所示	第三方网络能力可提供的网络能力 API 列表

表 6

数据类型	说明
String	每一种网络能力类型用字符串来表示，比如“NEF”、“CSMF”、“Location（即定位能力）”等
Numbers	每一种网络能力类型用编号来表示，比如 01 代表 NEF，02 代表 CSMF，03 代表定位能力等
Bitmap	用每一个 bit 位来标识一种网络能力类型，如 bit0 标识 NEF，bit1 标识 CSMF，bit2 标识定位能力等；bit 位值为 0 表示不支持该 bit 位标识的网络能力类型；bit 位值为 1 表示支持该 bit 位标识的网络能力类型

表 7

数据类型	说明
字符串列表（List of String）	每一个网络能力 API 用字符串来表示，比如“NEF-3GPP-TrafficInfluence-API”
编号列表（List of Number）	每一个网络能力 API 用编号来表示，比如 001 代表 NEF TrafficInfluence API，002 代表 CSMF NetworkSlicing

	API 等
Bitmap	用每一个 bit 位来标识一个网络能力 API，如 bit0 标识 NEF TrafficInfluence API，bit1 标识 CSMF NetworkSlicing API 等；bit 位为 0 表示不支持该 bit 位标识的网络能力 API；bit 为 1 表示支持该 bit 位标识的网络能力 API

表 8

参数名	数据类型	说明
认证结果	Boolean	认证成功或失败
错误原因	String	如果认证失败，返回错误码及错误原因描述
网络能力身份标识	如表 10 所示	如果认证成功，返回该第三方网络能力在通信系统内唯一的身份标识

表 9

数据类型	说明
String	网络能力身份标识用字符串来表示，比如“CMHWNEF002”
ID 编号	网络能力身份标识用 ID 编号来表示，比如 0102003065，该编号的第 1-2 位表示运营商、第 3-5 位表示设备提供商、第 6-7 位表示网络能力类型、第 8-10 位为通信系统的内部编号

表 10

实际应用时，列表（即 List of String 和 List of Number）可以理解为一维数组，用于存储同种类型的一系列数据。在不同编程语言中，列表可以是静态的，也可以是动态变化的。

2）基于接口 I2 实现第三方网络能力的接入控制功能时，行业网关可以通过接口 I2 向第三方网络能力发送接入控制信息（即上述第二信息），以实现对第三方网络能力的接入控制功能；所述接入控制信息包含的内容如表 11 所示。

参数名	数据类型	说明
网络能力身份标识	如表 10 所示	第三方网络能力在通信系统内唯一的身份标识
网络能力接入状态指示（On/ Off）	Boolean	第三方网络能力接入的开启或关闭指示

表 11

3）行业网关还可以通过接口 I2 从第三方网络能力获取网络能力数据，以实现面向 MEP 的网络能力开放。

第三，对接口 I3 承载的信息进行详细说明。

1）基于接口 I3 实现行业网关的接入认证功能时，行业网关可以通过接口 I3 向 BSS/OSS 发送身份认证信息；所述身份认证信息包含的内容如表

12 所示；其中，如表 13 所示，网络类型列表可以通过多种不同的数据类型表示；如表 14 所示，网络能力类型列表也可以通过多种不同的数据类型表示。BSS/OSS 完成行业网关的接入认证后，可以通过接口 I3 向行业网关返回认证响应信息；所述认证响应信息包含的内容如表 15 所示；其中，如表 16 所示，行业网关身份标识可以通过多种不同的数据类型表示。

参数名	数据类型	说明
用户名	String	具有行业网关注册权限的用户名
密钥	String	用户名对应的密钥
网络类型列表	如表 13 所示	行业网关支持接入的网络类型列表
网络能力类型列表	如表 14 所示	行业网关支持接入的网络能力类型列表
最大带宽	Number	行业网关所支持的最大带宽容量
带宽控制粒度	Number	行业网关所支持的带宽控制粒度

表 12

数据类型	说明
List of String	每一种网络类型用字符串来表示，比如“4G”、“WiFi6”、“Wireline”等；字符串列表表示行业网关所支持接入的网络类型列表
List of Number	每一种网络类型用编号来表示，比如 01 代表 4G，02 代表 Wireline，03 代表 WiFi 等；编号列表表示行业网关所支持接入的网络类型列表
Bitmap	用每一个 bit 位来标识一种网络类型，比如 bit0 标识 Wireline，bit1 标识 4G，bit2 标识 WiFi 等；bit 位值为 0 表示不包含该 bit 位标识的网络类型；bit 位值为 1 表示包含该 bit 位标识的网络类型

表 13

数据类型	说明
List of String	每一种网络能力类型用字符串来表示，比如“NEF”、“CSMF”、“Location”等；字符串列表表示行业网关所支持接入的网络能力类型列表
List of Number	每一种网络能力类型用编号来表示，比如 01 代表 NEF，02 代表 CSMF，03 代表定位能力等；编号列表表示行业网关所支持接入的网络能力类型列表
Bitmap	用每一个 bit 位来标识一种网络能力类型，比如 bit0 标识 NEF，bit1 标识 CSMF，bit2 标识定位能力等；bit 位值为 0 表示不包含该 bit 位标识的网络能力类型；bit 位值为 1 表示包含该 bit 位标识的网络能力类型

表 14

参数名	数据类型	说明
认证结果	Boolean	认证成功或失败
错误原因	String	如果认证失败，返回错误码及错误原因描述
行业网关身份标识	如表 16 所示	如果认证成功，返回该行业网关在通信系统内唯一的身份标识

表 15

数据类型	说明
String	行业网关身份标识用字符串来表示，比如“CMHWNEF096”
ID 编号	行业网关身份标识用 ID 编号来表示，比如 0102003031，该编号的第 1-2 位表示运营商、第 3-5 位表示设备提供商、第 6-7 位表示部署位置、第 8-10 位为通信系统的内部编号

表 16

2）基于接口 I3 实现第三方网络的接入控制功能时，BSS/OSS 可以通过接口 I3 向行业网关发送单个第三方网络接入控制策略（即上述第一接入控制策略），以实现对行业网关连接的单个第三方网络的接入控制功能；所述单个第三方网络接入控制策略包含的内容如表 17 所示。

参数名	数据类型	说明
行业网关身份标识	如表 16 所示	行业网关在通信系统内唯一的身份标识
网络身份标识	如表 4 所示	该第三方网络在通信系统内唯一的身份标识
最大带宽	Number	用于限制该第三方网络的最大接入带宽
最大流量	Number	用于限制该第三方网络的最大网络流量
接入时长	Number	用于限制该第三方网络的最长接入时长
最大接入用户数	Number	用于限制该第三方网络的最大接入用户数
计费策略	String	用于描述该第三方网络的计费策略；第三方网络的计费策略详见本应用实施例的后续描述
网络接入状态指示（On/ Off）	Boolean	该第三方网络接入的开启或关闭指示

表 17

实际应用时，BSS/OSS 也可以通过接口 I3 向行业网关发送单类型第三方网络接入控制策略（即上述第二接入控制策略），以实现对行业网关上单类型的第三方网络的接入控制功能；所述单类型第三方网络接入控制策略包含的内容如表 18 所示。

参数名	数据类型	说明

行业网关身份标识	如表 16 所示	行业网关在通信系统内唯一的身份标识
网络类型标识	如表 2 所示	表示第三方网络的网络类型
最大带宽	Number	用于限制该类型的第三方网络的最大接入带宽
最大流量	Number	用于限制该类型的第三方网络的最大网络流量
接入时长	Number	用于限制该类型的第三方网络的最长接入时长
最大接入用户数	Number	用于限制该类型的第三方网络的最大接入用户数
计费策略	String	用于描述该类型的第三方网络的计费策略；第三方网络的计费策略详见本应用实施例的后续描述
网络接入状态指示（On/ Off）	Boolean	该类型的第三方网络接入的开启或关闭指示

表 18

实际应用时，BSS/OSS 还可以通过接口 I3 向行业网关发送整体第三方网络接入控制策略（即上述第三接入控制策略），以实现对行业网关上所有第三方网络的接入控制功能；所述整体第三方网络接入控制策略包含的内容如表 19 所示。

参数名	数据类型	说明
行业网关身份标识	如表 16 所示	行业网关在通信系统内唯一的身份标识
最大带宽	Number	用于限制行业网关上所有第三方网络的最大接入带宽
最大流量	Number	用于限制行业网关上所有第三方网络的最大网络流量
接入时长	Number	用于限制行业网关上所有第三方网络的最长接入时长
最大接入用户数	Number	用于限制行业网关上所有第三方网络的最大接入用户数
计费策略	String	用于描述行业网关上所有第三方网络的计费策略；第三方网络的计费策略详见本应用实施例的后续描述
网络接入状态指示（On/ Off）	Boolean	行业网关上所有第三方网络接入的开启或关闭指示

表 19

在本应用实施例中，所述第三方网络的计费策略可以包含以下至少之

一：

按带宽计费；即按照第三方网络的最大带宽值计费，比如按带宽包年包月计费、按带宽使用时长计费等计费模式；

按流量计费；即按照第三方网络实际传输的数据总量计费；

按网络切片计费；即按照所使用的第三方网络切片的类型和数量计费；

按 QoS 计费；即按照第三方网络提供的 QoS 计费，比如数据传输速率、时延、抖动、可靠性等；

按接入用户数计费；即按照第三方网络接入的用户数计费，比如按最大接入用户数包月包年计费、按实际接入用户数计费等计费模式。

3）基于接口 I3 实现第三方网络能力的接入控制功能时，BSS/OSS 可以通过接口 I3 向行业网关发送单个第三方网络能力接入控制策略（即上述第四接入控制策略），以实现对行业网关上单个第三方网络能力的接入控制功能；所述单个第三方网络能力接入控制策略包含的内容如表 20 所示。

参数名	数据类型	说明
行业网关身份标识	如表 16 所示	行业网关在通信系统内唯一的身份标识
网络能力身份标识	如表 10 所示	该第三方网络能力在通信系统内唯一的身份标识
网络能力 API 最大调用次数	Number	用于限制行业网关对该第三方网络能力的 API 的最大调用次数
接入时长	Number	用于限制该第三方网络能力的最长接入时长
计费策略	String	用于描述该第三方网络能力的计费策略；第三方网络能力的计费策略详见本应用实施例的后续描述
网络能力接入状态指示（On/ Off）	Boolean	该第三方网络能力接入的开启或关闭指示

表 20

实际应用时，BSS/OSS 也可以通过接口 I3 向行业网关发送单类型第三方网络能力接入控制策略（即上述第五接入控制策略），以实现对行业网关上单类型的第三方网络能力的接入控制功能；所述单类型第三方网络能力接入控制策略包含的内容如表 21 所示。

参数名	数据类型	说明
行业网关身份标识	如表 16 所示	行业网关在通信系统内唯一的身份标识
网络能力类型标识	如表 7 所示	表示第三方网络能力的类型
网络能力 API 最大调用次数	Number	用于限制行业网关对该类型的第三方网络能力的 API 的最大调用次数
接入时长	Number	用于限制该类型的第三方网络能力的最

		长接入时长
计费策略	String	用于描述该类型的第三方网络能力的计费策略；第三方网络能力的计费策略详见本应用实施例的后续描述
网络能力接入状态指示（On/ Off）	Boolean	该类型的第三方网络能力接入的开启或关闭指示

表 21

实际应用时，BSS/OSS 还可以通过接口 I3 向行业网关发送整体第三方网络能力接入控制策略（即上述第六接入控制策略），以实现对行业网关上所有第三方网络能力的接入控制功能；所述整体第三方网络能力接入控制策略包含的内容如表 22 所示。

参数名	数据类型	说明
行业网关身份标识	如表 16 所示	行业网关在通信系统内唯一的身份标识
网络能力 API 最大调用次数	Number	用于限制行业网关对所有第三方网络能力的 API 的最大调用次数
接入时长	Number	用于限制行业网关上所有第三方网络能力的最长接入时长
计费策略	String	用于描述行业网关上所有第三方网络能力的计费策略；第三方网络能力的计费策略详见本应用实施例的后续描述
网络能力接入状态指示（On/ Off）	Boolean	行业网关上所有第三方网络能力接入的开启或关闭指示

表 22

在本应用实施例中，所述第三方网络能力的计费策略可以包含以下至少之一：

按第三方网络能力的 API 的实际调用次数计费；

按第三方网络能力的数据流量计费；即按照实际传输的网络能力数据总量计费；

按第三方网络能力的类型计费；即针对不同的第三方网络能力的类型，指定不同的计费模式及价格；

按第三方网络能力的数据来源计费；即针对不同的第三方网络能力的数据来源，指定不同的计费模式及价格；

4）基于接口 I3 实现 MEP 的接入控制功能时，BSS/OSS 可以通过接口 I3 向行业网关发送 MEP 接入控制策略（即上述第一策略），以实现对 MEP 的接入控制功能；所述 MEP 接入控制策略包含的内容如表 23 所示；其中，如表 24 所示，MEP 身份标识可以通过多种不同的数据类型表示；如表 25

所示，自服务网络安全管控 API 列表也可以通过多种不同的数据类型表示。

参数名	数据类型	说明
行业网关身份标识	如表 16 所示	行业网关在通信系统内唯一的身份标识
MEP 身份标识	如表 24 所示	MEP 在通信系统内唯一的身份标识
加密策略	String	用于描述 MEP 与行业网关之间的传输通道的加密策略
网络能力类型列表	如表 14 所示	该 MEP 允许访问的网络能力类型列表
网络能力 API 列表	如表 8 所示	该 MEP 允许访问的网络能力 API 列表
网络能力 API 最大调用次数	Number	用于限制该 MEP 对网络能力的 API 的最大调用次数
自服务网络安全管控 API 列表	如表 25 所示	该 MEP 允许访问的自服务网络安全管控 API 列表
MEP 接入状态指示（On/ Off）	Boolean	该 MEP 接入行业网关的开启或关闭指示
最大带宽	Number	限制行业网关与该 MEP 之间传输通道的最大带宽
最大流量	Number	限制行业网关与该 MEP 之间传输通道的最大流量

表 23

数据类型	说明
String	MEP 身份标识用字符串来表示，比如“CMHWHUAXI002”
ID 编号	MEP 身份标识用 ID 编号来表示，比如 0102003078，该编号的第 1-2 位表示运营商、第 3-5 位表示设备提供商、第 6-7 位表示部署位置、第 8-10 位为通信系统的内部编号

表 24

数据类型	说明
List of String	每一个自服务网络安全管控 API 用字符串来表示，比如“IGW-NETDOMAIN-API”
List of Number	每一个自服务网络安全管控 API 用编号来表示，比如 001 代表 NetworkDomain API，002 代表 NetworkQoS API 等
Bitmap	用每一个 bit 位来标识一个自服务网络安全管控 API，如 bit0 标识 NetworkDomain API，bit1 标识 NetworkQoS API 等；bit 位为 0 表示不支持该 bit 位标识的自服务网络安全管控 API；bit 位值为 1 表示支持该 bit 位标识的

	自服务网络安全管控 API

表 25

5）基于接口 I3 实现网络状态监控功能时，行业网关可以通过接口 I3 向 BSS/OSS 发送网络状态监控信息，以实现网络状态监控功能；所述网络状态监控信息包含的内容如表 26 所示；其中，如表 27 所示，第三方网络状态统计信息、第三方网络能力状态统计信息和 MEP 状态统计信息可以通过多种不同的数据类型表示。

参数名	数据类型	说明
行业网关身份标识	如表 16 所示	行业网关在通信系统内唯一的身份标识
统计时间周期	时期（Period）	本次网络状态监控对应的统计时间周期
第三方网络状态统计信息	如表 27 所示	每一个第三方网络的状态监控统计信息，包括网络身份标识、网络类型标识、吞吐率、流量、接入时长等
第三方网络能力状态统计信息	如表 27 所示	每一个第三方网络能力的状态监控统计信息，包括网络能力身份标识、网络能力类型标识、API 调用次数、流量、接入时长等
MEP 状态统计信息	如表 27 所示	每一个 MEP 的状态监控统计信息，包括 MEP 身份标识、吞吐率、流量、网络能力 API 调用次数、接入时长等
计费明细	String	依据第三方网络及第三方网络能力的计费策略所计算与生成的计费明细

表 26

数据类型	说明
键值对列表（List of “key-value” pairs）	所统计信息的名称与数值对的列表，比如，数据吞吐率=20Mbps、网络能力 API 调用次数=1000 等
固定结构（Structure）	固定定义统计信息各字节的含义，比如，字节 1-2 代表吞吐率的数值

表 27

第四，对接口 I4 承载的信息进行详细说明。

1）基于接口 I4 实现 MEP 的接入认证功能时，MEP 可以通过接口 I4 向行业网关发送 MEP 接入认证信息；所述 MEP 接入认证信息包含的内容如表 28 所示。行业网关完成对 MEP 的认证后，可以通过接口 I4 返回 MEP 接入认证响应信息；所述 MEP 接入认证响应信息包含的内容如表 29 所示。

参数名	数据类型	说明

用户名	String	具有 MEP 注册权限的用户名
密钥	String	用户名对应的密钥
MEP 特征	String	用于描述 MEP 的特征，比如 MEP 的 IP 地址段、MEP 所承载的应用、MEP 的业务优先级等

表 28

参数名	数据类型	说明
认证结果	Boolean	认证成功或失败
错误原因	String	如果认证失败，返回错误码及错误原因描述
MEP 身份标识	如表 24 所示	如果认证成功，返回该 MEP 在通信系统内唯一的身份标识

表 29

2）基于接口 I4 实现 MEP 的接入控制功能时，行业网关可以通过接口 I4 向 MEP 发送 MEP 接入控制信息（即上述第三信息），以实现对 MEP 的接入控制功能；所述 MEP 接入控制信息包含的内容如表 30 所示。

参数名	数据类型	说明
MEP 身份标识	如表 24 所示	该 MEP 在通信系统内唯一的身份标识
MEP 接入状态指示（On/ Off）	Boolean	该 MEP 接入行业网关的开启或关闭指示
网络能力 API 列表	如表 8 所示	该 MEP 可访问（即允许访问）的网络能力 API 列表
自服务网络安全管控 API 列表	如表 25 所示	该 MEP 可访问的自服务网络安全管控 API 列表

表 30

4）基于接口 I4 实现面向 MEP 的网络能力开放功能时，MEP 可以通过行业网关开放的网络能力 API，获取网络能力开放数据；此时，MEP 与行业网关交互的信息所包含的内容如表 31 所示。。

参数名	数据类型	说明
MEP 身份标识	如表 24 所示	MEP 在通信系统内唯一的身份标识
网络数据能力	String 或 Structure	符合网络能力 API 定义的网络能力数据，可以包括定位能力标签（比如 5G、WiFi、Bluetooth、GPS 等）、定位数据、接入用户信息、第三方网络接入列表、网络切片能力数据、QoS 能力数据等

表 31

5）基于接口 I4 实现面向 MEP 的自服务网络安全管控功能时，MEP 可

以通过行业网关开放的自服务网络安全管控 API，获取网络能力开放数据；此时，MEP 与行业网关交互的信息所包含的内容如表 32 所示。

参数名	数据类型	说明
MEP 身份标识	如表 24 所示	MEP 在通信系统内唯一的身份标识
自服务网络安全管控指令（即上述第一指令）	String 或 Structure	符合自服务网络安全管控 API 定义的指令，可以包括网络分区权限管理、网络性能要求、业务路由策略、网络切片模板配置、定位区域大小及位置配置、接入用户 ID 配置（手机号码、用户名或者应用 ID）等

表 32

第五，对接口 I5 承载的信息进行详细说明。

基于接口 I5 实现行业网关之间的广域互联功能时，不同行业网关之间可以通过 SD-WAN、互联网、企业专线、无线网络等方式建立互联通道，实现广域互联功能。

在本应用实施例中，行业网关支持的功能接受 BSS/OSS 的统一管控，该管控通过接口 I3 与其他接口的联动（即结合）来实现。下面结合图 7 至图 10 描述接口 I3 与其他接口联动实现相应功能的流程。

首先，基于接口 I3 与接口 I1 的联动，可以实现行业网关对第三方网络的接入认证功能和接入控制功能，如图 7 所示，实现行业网关对第三方网络的接入认证功能的过程具体可以包括以下步骤：

步骤 7101：第三方网络通过接口 I1 向行业网关发送第三方网络接入认证信息；之后执行步骤 7102；

步骤 7102：行业网关通过接口 I3 将第三方网络接入认证信息发送到 BSS/OSS；之后执行步骤 7103；

步骤 7103：BSS/OSS 实施对第三方网络的接入认证；之后执行步骤 7104；

步骤 7104：BSS/OSS 通过接口 I3 向行业网关发送包含认证结果的第三方网络接入认证响应信息；之后执行步骤 7105；

步骤 7105：行业网关通过接口 I1 向第三方网络发送第三方网络接入认证响应信息。

实现行业网关对第三方网络的接入控制功能的过程具体可以包括以下步骤：

步骤 7201：BSS/OSS 通过接口 I3 向行业网关发送第三方网络接入控制策略；之后执行步骤 7202；

步骤 7202：行业网关根据第三方网络接入控制策略（即上述第二策略），实施对第三方网络的接入控制；之后执行步骤 7203；

这里，行业网关实施的对第三方网络的接入控制，可以包括带宽限制、接入用户数限制、第三方网络接入的开启或关闭、计费等；

步骤 7203：行业网关通过接口 I1 向第三方网络发送第三方网络接入控制信息（即上述第一信息）。

其次，基于接口 I3 与接口 I2 的联动，可以实现行业网关对第三方网络能力的接入认证功能和接入控制功能，如图 8 所示，实现行业网关对第三方网络能力的接入认证功能的过程具体可以包括以下步骤：

步骤 8101：第三方网络能力通过接口 I2 向行业网关发送第三方网络能力接入认证信息；之后执行步骤 8102；

步骤 8102：行业网关将第三方网络能力接入认证信息通过接口 I3 发送到 BSS/OSS；之后执行步骤 8103；

步骤 8103：BSS/OSS 实施对第三方网络能力的接入认证；之后执行步骤 8104；

步骤 8104：BSS/OSS 通过接口 I3 向行业网关发送包含认证结果的第三方网络能力接入认证响应信息；之后执行步骤 8105；

步骤 8105：行业网关通过接口 I2 向第三方网络能力发送第三方网络能力接入认证响应信息。

实现行业网关对第三方网络能力的接入控制功能的过程具体可以包括以下步骤：

步骤 8201：BSS/OSS 通过接口 I3 向行业网关发送第三方网络能力接入控制策略（即上述第三策略）；之后执行步骤 8202；

步骤 8202：行业网关根据第三方网络能力接入控制策略，实施对第三方网络能力的接入控制；之后执行步骤 8203；

这里，行业网关实施的对第三方网络能力的接入控制可以包括网络能力 API 调用次数限制、第三方网络能力接入的开启或关闭、计费等；

步骤 8203：行业网关通过接口 I2 向第三方网络能力发送第三方网络能力接入控制信息（即上述第二信息）。

第三，基于接口 I3 与接口 I4 的联动，可以实现行业网关对 MEP 的接入认证功能和接入控制功能，如图 9 所示，实现行业网关对 MEP 的接入认证功能的过程具体可以包括以下步骤：

步骤 9101：MEP 通过接口 I4 向行业网关发送 MEP 接入认证信息；之后执行步骤 9102；

步骤 9102：行业网关将 MEP 接入认证信息通过接口 I3 发送到 BSS/OSS；之后执行步骤 9103；

步骤 9103：BSS/OSS 实施对 MEP 的接入认证；之后执行步骤 9104；

步骤 9104：BSS/OSS 通过接口 I3 向行业网关发送包含认证结果的 MEP 接入认证响应信息；之后执行步骤 9105；

步骤 9105：行业网关通过接口 I4 向 MEP 发送 MEP 接入认证响应信息。

实现行业网关对 MEP 的接入控制功能的过程具体可以包括以下步骤：

步骤 9201：BSS/OSS 通过接口 I3 向行业网关发送 MEP 接入控制策略

（即上述第一策略）；之后执行步骤 9202；

步骤 9202：行业网关根据 MEP 接入控制策略，实施对 MEP 的接入控制；之后执行步骤 9203；

这里，行业网关实施的对 MEP 的接入控制可以包括允许访问的网络能力限制、带宽限制、计费等；

步骤 9103：行业网关通过接口 I4 向 MEP 发送 MEP 接入控制信息（即上述第三信息）。

第四，基于接口 I3、接口 I4、接口 I1 和接口 I2 的联动，可以实现面向 MEP 的网络能力开放功能和自服务网络安全管控功能，如图 10 所示，实现面向 MEP 的网络能力开放功能的过程具体可以包括以下步骤：

步骤 1011：BSS/OSS 通过接口 I3 向行业网关下发 MEP 接入控制策略（即上述第一策略）；之后执行步骤 1012；

这里，所述 MEP 接入控制策略包含面向 MEP 的网络能力开放相关的控制策略；

步骤 1012：MEP 通过接口 I4 调用行业网关的网络能力开放 API；之后执行步骤 1013；

步骤 1013：行业网关根据 MEP 接入控制策略对 MEP 的请求进行校验，校验通过后，行业网关通过接口 I2 向第三方网络能力发送获取网络能力数据的请求；之后执行步骤 1014；

这里，行业网关可以校验 MEP 的请求是否不属于相应 MEP 允许访问的网络能力；或者，可以校验 MEP 的请求是否超出了相应 MEP 允许调用的网络能力开放 API 次数等；

步骤 1014：第三方网络能力通过接口 I2 向行业网关发送网络能力数据；之后执行步骤 1015；

步骤 1015：行业网关通过接口 I4 将网络能力数据发送给 MEP。

实现面向 MEP 的自服务网络安全管控功能的过程具体可以包括以下步骤：

步骤 1011：BSS/OSS 通过接口 I3 向行业网关下发 MEP 接入控制策略；之后执行步骤 1021；

这里，所述 MEP 接入控制策略包含面向 MEP 的自服务网络安全管控相关的控制策略；

步骤 1021：MEP 通过接口 I4 调用行业网关的自服务网络安全管控 API；之后执行步骤 1022；

步骤 1022：行业网关根据 MEP 接入控制策略对 MEP 的请求进行校验，校验通过后，行业网关通过接口 I1 向第三方网络发送自服务网络管控指令（即上述第一指令）；之后执行步骤 1023；

这里，行业网关可以校验 MEP 的请求是否不属于 MEP 允许访问的自服务网络安全管控 API；所述自服务网络管控指令可以是网络安全管控指

令;

步骤 1023: 第三方网络通过接口 I1 向行业网关发送自服务网络管控结果; 之后执行步骤 1024;

这里, 在所述自服务网络管控指令是网络安全管控指令的情况下, 所述自服务网络管控结果为网络安全管控结果;

步骤 1024: 行业网关通过接口 I4 将自服务网络管控响应信息发送给 MEP。

本应用实施例提供的方案, 具有以下优点:

本应用实施例提供的方案, 在相关技术的基础上, 将行业网关(可以是网络设备或网元)引入通信系统, 部署在 UPF 与 MEP 之间, 并接受 BSS/OSS 的管理与控制; 行业网关至少具备多制式网络接入控制、网络智能广域互联、多类型网络能力接入与开放、多制式网络监控与计费、自服务资源管理等方面的功能; 同时, 基于全新定义的 5 个接口(接口 I1 至 I5)实现了上述功能; 其中, 接口 I1 对接多制式接入网络(即第三方网络); 接口 I2 对接多类型网络能力的接入(即第三方网络能力); 接口 I3 对接 BSS/OSS; 接口 I4 对接 MEP; 接口 I5 对接其他的行业网关。

基于所述行业网关的应用, 本应用实施例提供的通信系统(即 5G 行业云网融合的系统)可运营、更安全、可落地、可演进, 更加贴合垂直行业客户需求。具体地, 通过本应用实施例提供的方案, 一方面, 能够解决相关技术(即图 1 所示的 5G 与 MEC 技术结合方案)在行业落地中存在的 UPF 与 MEC 分离部署带来的网络和计算资源安全问题、不支持多制式网络(比如 4G、5G、WiFi、Bluetooth、Zigbee、NB-IoT、光纤、Wireline 等)的接入与统一管理问题、本地分流的缺陷问题和 MEP 之间的互联互通等问题; 另一方面, 能够满足用户对多样化的网络能力开放和自服务资源管理能力等方面的需求。

为了实现本申请实施例的方法, 本申请实施例还提供了一种通信装置, 设置在第一设备上, 如图 11 所示, 该装置包括:

处理单元 1101, 配置为为 UPF 发送的边缘网络的业务流量分配对应的第二设备, 以将边缘网络的业务流量分流至对应的第二设备, 并为第二设备提供的应用提供安全访问控制功能。

其中, 在一实施例中, 所述处理单元 1101, 还配置为对连接的第二设备进行接入认证。

在一实施例中, 如图 11 所示, 该装置还包括控制单元 1102, 配置为控制第二设备对网络能力的访问。

在一实施例中, 所述处理单元 1101, 配置为:

接收所述第二设备发送的接入认证信息;

将所述接入认证信息发送给第三设备;

接收到所述第三设备返回的认证响应信息后, 向所述第二设备返回认

证响应信息。

在一实施例中，所述处理单元 1101，还配置为：

接收第三设备发送的第一策略；

基于所述第一策略为第二设备提供的应用提供安全访问控制功能，和/或，基于所述第一策略控制第二设备对网络能力的访问。

在一实施例中，所述处理单元 1101，还配置为为接入第三方网络的终端选择对应的第二设备，将对应第二设备提供的应用通过所述第三方网络提供给所述终端。

在一实施例中，所述处理单元 1101，还配置为对所述第三方网络进行接入认证。

在一实施例中，所述处理单元 1101，配置为：

接收所述第三方网络发送的接入认证信息；

将所述接入认证信息发送给所述第三设备；

接收到所述第三设备返回的认证响应信息后，向所述第三方网络返回认证响应信息。

在一实施例中，所述处理单元 1101，还配置为在接入认证通过后，基于安全机制与所述第三方网络进行数据传输。

在一实施例中，所述控制单元 1102，还配置为控制所述第三方网络的接入能力。

在一实施例中，所述控制单元 1102，配置为：

接收第三设备发送的第二策略；

基于所述第二策略控制所述第三方网络的接入能力。

在一实施例中，所述处理单元 1101，配置为向所述第三方网络发送第一信息，所述第一信息用于指示所述第三方网络的接入能力。

在一实施例中，所述处理单元 1101，还配置为接收第四设备发送的网络能力信息。

在一实施例中，所述控制单元 1102，还配置为控制所述第四设备的接入能力。

在一实施例中，所述处理单元 1101，还配置为对第四设备进行接入认证。

在一实施例中，所述处理单元 1101，配置为向所述第四设备发送第二信息，所述第二信息用于指示所述第四设备的接入能力。

在一实施例中，所述控制单元 1102，配置为：

接收所述第三设备发送的第三策略；

基于所述第三策略控制所述第四设备的接入能力。

在一实施例中，所述处理单元 1101，配置为：

接收所述第四设备发送的接入认证信息；

将所述接入认证信息发送给第三设备；

接收到所述第三设备返回的认证响应信息后，向所述第四设备返回认证响应信息。

在一实施例中，所述处理单元 1101，还配置为通过至少一个其他第一设备，将终端的业务流进行路由转发，以实现所述终端获取至少一个其他第一设备连接的第二设备提供的应用。

在一实施例中，所述处理单元 1101，还配置为监控网络的流量和/或网络状态；并向第三设备上报以下信息至少之一：

网络的流量；

计费信息；

网络状态的监控信息；

网络能力的使用信息；

第二设备状态的监控信息。

在一实施例中，该装置还包括获取单元，配置为获取至少一个网络（包含 5G 网络和/或第三方网络）的网络信息，以提供给需要的设备（比如 MEAO）。

在一实施例中，所述获取单元，配置为从第三方网络的管理设备获得第三方网络的网络信息，和/或，从 5G 的管理设备获得 5G 网络的网络信息。

实际应用时，所述处理单元 1101、所述控制单元 1102 及所述获取单元可由通信装置中的处理器结合通信接口实现。

需要说明的是：上述实施例提供的通信装置在进行通信时，仅以上述各程序模块的划分进行举例说明，实际应用中，可以根据需要而将上述处理分配由不同的程序模块完成，即将装置的内部结构划分成不同的程序模块，以完成以上描述的全部或者部分处理。另外，上述实施例提供的通信装置与通信方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

基于上述程序模块的硬件实现，且为了实现本申请实施例的方法，本申请实施例还提供了一种第一设备，如图 12 所示，该第一设备 1200 包括：处理器 1202 及通信接口 1201；其中，

所述处理器 1202，配置为为 UPF 发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。

其中，在一实施例中，所述处理器 1202，还配置为：

对连接的第二设备进行接入认证；

和/或，

控制第二设备对网络能力的访问。

在一实施例中，所述处理器 1202，配置为：

通过所述通信接口 1201 接收所述第二设备发送的接入认证信息；

通过所述通信接口 1201 将所述接入认证信息发送给第三设备；

通过所述通信接口 1201 接收到所述第三设备返回的认证响应信息后，通过所述通信接口 1201 向所述第二设备返回认证响应信息。

在一实施例中，所述处理器 1202，还配置为：

通过所述通信接口 1201 接收第三设备发送的第一策略；

基于所述第一策略为第二设备提供的应用提供安全访问控制功能，和/或，基于所述第一策略控制第二设备对网络能力的访问。

在一实施例中，所述处理器 1202，还配置为为接入第三方网络的终端选择对应的第二设备，将对应第二设备提供的应用通过所述第三方网络提供给所述终端。

在一实施例中，所述处理器 1202，还配置为对所述第三方网络进行接入认证。

在一实施例中，所述处理器 1202，配置为：

通过所述通信接口 1201 接收所述第三方网络发送的接入认证信息；

通过所述通信接口 1201 将所述接入认证信息发送给所述第三设备；

通过所述通信接口 1201 接收到所述第三设备返回的认证响应信息后，通过所述通信接口 1201 向所述第三方网络返回认证响应信息。

在一实施例中，所述处理器 1202，还配置为在接入认证通过后，基于安全机制与所述第三方网络进行数据传输。

在一实施例中，所述处理器 1202，还配置为控制所述第三方网络的接入能力。

在一实施例中，所述处理器 1202，还配置为：

通过所述通信接口 1201 接收第三设备发送的第二策略；

基于所述第二策略控制所述第三方网络的接入能力。

在一实施例中，所述处理器 1202，配置为通过所述通信接口 1201 向所述第三方网络发送第一信息，所述第一信息用于指示所述第三方网络的接入能力。

在一实施例中，所述处理器 1202，还配置为通过所述通信接口 1201 接收第四设备发送的网络能力信息。

在一实施例中，所述处理器 1202，还配置为：

控制所述第四设备的接入能力；

和/或，

对第四设备进行接入认证。

在一实施例中，所述处理器 1202，配置为通过所述通信接口 1201 向所述第四设备发送第二信息，所述第二信息用于指示所述第四设备的接入能力。

在一实施例中，所述处理器 1202，还配置为：

通过所述通信接口 1201 接收所述第三设备发送的第三策略；

基于所述第三策略控制所述第四设备的接入能力。

在一实施例中，所述处理器 1202，配置为：

通过所述通信接口 1201 接收所述第四设备发送的接入认证信息；

通过所述通信接口 1201 将所述接入认证信息发送给第三设备；

通过所述通信接口 1201 接收到所述第三设备返回的认证响应信息后，通过所述通信接口 1201 向所述第四设备返回认证响应信息。

在一实施例中，所述处理器 1202，还配置为通过至少一个其他第一设备，将终端的业务流进行路由转发，以实现所述终端获取至少一个其他第一设备连接的第二设备提供的应用。

在一实施例中，所述处理器 1202，还配置为监控网络的流量和/或网络状态；并通过所述通信接口 1201 向第三设备上报以下信息至少之一：

网络的流量；

计费信息；

网络状态的监控信息；

网络能力的使用信息；

第二设备状态的监控信息。

在一实施例中，所述处理器 1202，还配置为通过所述通信接口 1201 获取至少一个网络（包含 5G 网络和/或第三方网络）的网络信息，以提供给需要的设备（比如 MEAO）。

在一实施例中，所述处理器 1202，配置为通过所述通信接口 1201 从第三方网络的管理设备获得第三方网络的网络信息，和/或，通过所述通信接口 1201 从 5G 的管理设备获得 5G 网络的网络信息。

需要说明的是：所述通信接口 1201 和所述处理器 1202 的具体处理过程可参照上述方法理解。

当然，实际应用时，第一设备 1200 中的各个组件通过总线系统 1204 耦合在一起。可理解，总线系统 1204 用于实现这些组件之间的连接通信。总线系统 1204 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 12 中将各种总线都标为总线系统 1204。

本申请实施例中的存储器 1203 用于存储各种类型的数据以支持第一设备 1200 的操作。这些数据的示例包括：用于在第一设备 1200 上操作的任何计算机程序。

上述本申请实施例揭示的方法可以应用于所述处理器 1202 中，或者由所述处理器 1202 实现。所述处理器 1202 可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过所述处理器 1202 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的所述处理器 1202 可以是通用处理器、数字信号处理器（DSP，Digital Signal Processor），或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。所述处理器 1202 可以实现或者执行本申请实施例中的公开的各方法、步骤

及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤，可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中，该存储介质位于存储器 1203，所述处理器 1202 读取存储器 1203 中的信息，结合其硬件完成前述方法的步骤。

在示例性实施例中，第一设备 1200 可以被一个或多个应用专用集成电路（ASIC，Application Specific Integrated Circuit）、DSP、可编程逻辑器件（PLD，Programmable Logic Device）、复杂可编程逻辑器件（CPLD，Complex Programmable Logic Device）、现场可编程门阵列（FPGA，Field-Programmable Gate Array）、通用处理器、控制器、微控制器（MCU，Micro Controller Unit）、微处理器（Microprocessor）、或者其他电子元件实现，用于执行前述方法。

可以理解，本申请实施例中的存储器 1203 可以是易失性存储器或者非易失性存储器，也可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（ROM，Read Only Memory）、可编程只读存储器（PROM，Programmable Read-Only Memory）、可擦除可编程只读存储器（EPROM，Erasable Programmable Read-Only Memory）、电可擦除可编程只读存储器（EEPROM，Electrically Erasable Programmable Read-Only Memory）、磁性随机存取存储器（FRAM，ferromagnetic random access memory）、快闪存储器（Flash Memory）、磁表面存储器、光盘、或只读光盘（CD-ROM，Compact Disc Read-Only Memory）；磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器（RAM，Random Access Memory），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器（SRAM，Static Random Access Memory）、同步静态随机存取存储器（SSRAM，Synchronous Static Random Access Memory）、动态随机存取存储器（DRAM，Dynamic Random Access Memory）、同步动态随机存取存储器（SDRAM，Synchronous Dynamic Random Access Memory）、双倍数据速率同步动态随机存取存储器（DDRSDRAM，Double Data Rate Synchronous Dynamic Random Access Memory）、增强型同步动态随机存取存储器（ESDRAM，Enhanced Synchronous Dynamic Random Access Memory）、同步连接动态随机存取存储器（SLDRAM，SyncLink Dynamic Random Access Memory）、直接内存总线随机存取存储器（DRRAM，Direct Rambus Random Access Memory）。本申请实施例描述的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

在示例性实施例中，本申请实施例还提供了一种存储介质，即计算机存储介质，具体为计算机可读存储介质，例如包括存储计算机程序的存储器 1203，上述计算机程序可由第一设备 1200 的处理器 1202 执行，以完成前述方法所述步骤。计算机可读存储介质可以是 FRAM、ROM、PROM、

EPROM、EEPROM、Flash Memory、磁表面存储器、光盘、或 CD-ROM 等存储器。

需要说明的是：“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

另外，本申请实施例所记载的技术方案之间，在不冲突的情况下，可以任意组合。

以上所述，仅为本申请的较佳实施例而已，并非用于限定本申请的保护范围。

权利要求书

1、一种通信系统，包括：至少一个第一设备、至少一个第二设备、至少一个用户面功能 UPF；其中，

每个第一设备连接至少一个第二设备；每个第一设备连接至少一个 UPF；

所述第一设备，配置为为 UPF 发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。

2、根据权利要求 1 所述的系统，其中，所述第一设备，还配置为对连接的第二设备进行接入认证。

3、根据权利要求 2 所述的系统，其中，所述系统还包括：第三设备；其中，

所述第二设备，配置为向所述第一设备发送接入认证信息；接收所述第一设备返回的认证响应信息；

所述第一设备，配置为接收所述第二设备发送的接入认证信息，将所述接入认证信息发送给所述第三设备，接收所述第三设备返回的认证响应信息，以及向所述第二设备返回认证响应信息；

所述第三设备，配置为接收所述第一设备发送的接入认证信息，利用所述接入认证信息对所述第二设备进行接入认证，并向所述第一设备返回认证响应信息。

4、根据权利要求 3 所述的系统，其中，所述接入认证信息包含所述第二设备的特征。

5、根据权利要求 4 所述的系统，其中，所述特征包含以下至少之一：

IP 地址段；

承载的应用；

业务优先级。

6、根据权利要求 3 所述的系统，其中，所述第一设备，还配置为控制第二设备对网络能力的访问。

7、根据权利要求 6 所述的系统，其中，

所述第三设备，还配置为向所述第一设备发送第一策略；

所述第一设备，还配置为接收所述第三设备发送的第一策略，基于所述第一策略为第二设备提供的应用提供安全访问控制功能，和/或，基于所述第一策略控制第二设备对网络能力的访问。

8、根据权利要求 1 所述的系统，其中，所述系统还包括：至少一个第三方网络；其中，

所述第三方网络，配置为为终端提供网络接入；

所述第一设备，还配置为为所述终端选择对应的第二设备，并将对应第二设备提供的应用通过所述第三方网络提供给所述终端。

9、根据权利要求 8 所述的系统，其中，所述第一设备，还配置为对第三方网络进行接入认证。

10、根据权利要求 9 所述的系统，其中，所述系统还包括：第三设备；其中，

所述第三方网络，配置为向所述第一设备发送接入认证信息；并接收所述第一设备返回的认证响应信息；

所述第一设备，配置为接收所述第三方网络发送的接入认证信息，将所述接入认证信息发送给所述第三设备，接收所述第三设备返回的认证响应信息，以及向所述第三方网络返回认证响应信息；

所述第三设备，配置为接收所述第一设备发送的接入认证信息，利用所述接入认证信息对所述第三方网络进行接入认证，并向所述第一设备返回认证响应信息。

11、根据权利要求 10 所述的系统，其中，所述接入认证信息包含第三方网络的特征。

12、根据权利要求 11 所述的系统，其中，所述特征包含以下至少之一：

最大带宽；

带宽控制粒度；

IP 地址段；

业务优先级；

承载的应用。

13、根据权利要求 9 所述的系统，其中，所述第一设备，配置为接入认证通过后，基于安全机制与所述第三方网络进行数据传输。

14、根据权利要求 10 所述的系统，其中，所述第一设备，还配置为控制所述第三方网络的接入能力。

15、根据权利要求 14 所述的系统，其中，

所述第三设备，还配置为向所述第一设备发送第二策略；

所述第一设备，还配置为接收所述第三设备发送的第二策略，基于所述第二策略控制所述第三方网络的接入能力。

16、根据权利要求 15 所述的系统，其中，所述第二策略包含以下之一：

第一接入控制策略；所述第一接入控制策略针对单个第三方网络；

第二接入控制策略；所述第二接入控制策略针对一种类型的第三方网络；

第三接入控制策略；所述第三接入控制策略针对所有第三方网络。

17、根据权利要求 14 所述的系统，其中，所述第一设备，配置为向

所述第三方网络发送第一信息，所述第一信息用于指示所述第三方网络的接入能力；

所述第三方网络，配置为接收所述第一设备发送的第一信息，利用所述第一信息调整自身的接入能力。

18、根据权利要求 1 所述的系统，其中，所述系统还包括：至少一个第四设备；其中，

所述第四设备，配置为为所述第一设备提供网络能力信息。

19、根据权利要求 18 所述的系统，其中，所述第一设备，还配置为对第四设备进行接入认证。

20、根据权利要求 19 所述的系统，其中，所述系统还包括：第三设备；其中，

所述第四设备，还配置为向所述第一设备发送接入认证信息；接收所述第一设备返回的认证响应信息；

所述第一设备，配置为接收所述第四设备发送的接入认证信息，将所述接入认证信息发送给所述第三设备，接收所述第三设备返回的认证响应信息，以及向所述第四设备返回认证响应信息；

所述第三设备，配置为利用所述接入认证信息对所述第四设备进行接入认证，并向所述第一设备返回认证响应信息。

21、根据权利要求 20 所述的系统，其中，

所述第一设备，还配置为控制所述第四设备的接入能力。

22、根据权利要求 21 所述的系统，其中，所述第一设备，配置为向所述第四设备发送第二信息，所述第二信息用于指示所述第四设备的接入能力；

所述第四设备，配置为接收所述第一设备发送的第二信息，利用所述第二信息调整自身的接入能力。

23、根据权利要求 20 所述的系统，其中，

所述第三设备，还配置为向所述第一设备发送第三策略；

所述第一设备，还配置为接收所述第三设备发送的第三策略，并基于所述第三策略控制所述第四设备的接入能力。

24、根据权利要求 1 所述的系统，其中，所述第一设备，配置为通过至少一个其他第一设备，将终端的业务流进行路由转发，以实现所述终端获取至少一个其他第一设备连接的第二设备提供的应用。

25、根据权利要求 1 至 24 任一项所述的系统，其中，所述系统还包括：第三设备，配置为控制所述至少一个第一设备。

26、根据权利要求 25 所述的系统，其中，所述第三设备，还配置为对所述至少一个第一设备进行认证。

27、根据权利要求 26 所述的系统，其中，

所述第一设备，配置为向所述第三设备发送认证信息；并接收所述

第三设备返回的认证响应信息;

所述第三设备，配置为接收所述第一设备发送的认证信息，并利用所述认证信息对所述第一设备进行认证，并向所述第一设备返回认证响应信息。

28、根据权利要求 25 所述的系统，其中，所述第一设备，还配置为监控网络的流量和/或网络状态；并向所述第三设备上报以下信息至少之一:

网络的流量;

计费信息;

网络状态的监控信息;

网络能力的使用信息;

第二设备状态的监控信息。

29、一种通信方法，应用于第一设备，包括:

为 UPF 发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。

30、根据权利要求 29 所述的方法，其中，所述方法还包括:

对连接的第二设备进行接入认证;

和/或，

控制第二设备对网络能力的访问。

31、根据权利要求 30 所述的方法，其中，所述对连接的第二设备进行接入认证，包括:

接收所述第二设备发送的接入认证信息;

将所述接入认证信息发送给第三设备;

接收到所述第三设备返回的认证响应信息后，向所述第二设备返回认证响应信息。

32、根据权利要求 31 所述的方法，其中，所述接入认证信息包含所述第二设备的特征。

33、根据权利要求 32 所述的方法，其中，所述特征包含以下至少之一:

IP 地址段;

承载的应用;

业务优先级。

34、根据权利要求 30 所述的方法，其中，所述方法还包括:

接收第三设备发送的第一策略;

基于所述第一策略为第二设备提供的应用提供安全访问控制功能，和/或，基于所述第一策略控制第二设备对网络能力的访问。

35、根据权利要求 29 所述的方法，其中，所述方法还包括:

为接入第三方网络的终端选择对应的第二设备，将对应第二设备提供的应用通过所述第三方网络提供给所述终端。

36、根据权利要求 35 所述的方法，其中，所述方法还包括:

对所述第三方网络进行接入认证。

37、根据权利要求 36 所述的方法，其中，所述对所述第三方网络进行接入认证，包括:

接收所述第三方网络发送的接入认证信息;

将所述接入认证信息发送给所述第三设备;

接收到所述第三设备返回的认证响应信息后，向所述第三方网络返回认证响应信息。

38、根据权利要求 37 所述的方法，其中，所述接入认证信息包含第三方网络的特征。

39、根据权利要求 38 所述的方法，其中，所述特征包含以下至少之一:

最大带宽;

带宽控制粒度;

IP 地址段;

业务优先级;

承载的应用。

40、根据权利要求 37 所述的方法，其中，

接入认证通过后，基于安全机制与所述第三方网络进行数据传输。

41、根据权利要求 35 所述的方法，其中，所述方法还包括:

控制所述第三方网络的接入能力。

42、根据权利要求 41 所述的方法，其中，所述方法还包括:

接收第三设备发送的第二策略;

基于所述第二策略控制所述第三方网络的接入能力。

43、根据权利要求 42 所述的方法，其中，所述第二策略包含以下之一:

第一接入控制策略; 所述第一接入控制策略针对单个第三方网络;

第二接入控制策略; 所述第二接入控制策略针对一种类型的第三方网络;

第三接入控制策略; 所述第三接入控制策略针对所有第三方网络。

44、根据权利要求 41 所述的方法，其中，所述控制所述第三方网络的接入能力，包括:

向所述第三方网络发送第一信息，所述第一信息用于指示所述第三方网络的接入能力。

45、根据权利要求 29 所述的方法，其中，所述方法还包括:

接收第四设备发送的网络能力信息。

46、根据权利要求 45 所述的方法，其中，所述方法还包括:

控制所述第四设备的接入能力;

和/或，

对第四设备进行接入认证。

47、根据权利要求 46 所述的方法，其中，所述控制所述第四设备的接入能力，包括:

向所述第四设备发送第二信息，所述第二信息用于指示所述第四设备的接入能力。

48、根据权利要求 46 所述的方法，其中，所述方法还包括:

接收所述第三设备发送的第三策略;

基于所述第三策略控制所述第四设备的接入能力。

49、根据权利要求 46 所述的方法，其中，所述对第四设备进行接入认证，包括:

接收所述第四设备发送的接入认证信息;

将所述接入认证信息发送给第三设备;

接收到所述第三设备返回的认证响应信息后，向所述第四设备返回认证响应信息。

50、根据权利要求 29 所述的方法，其中，所述方法还包括:

通过至少一个其他第一设备，将终端的业务流进行路由转发，以实现所述终端获取至少一个其他第一设备连接的第二设备提供的应用。

51、根据权利要求 29 至 50 任一项所述的方法，其中，所述方法还包括:

监控网络的流量和/或网络状态; 并向第三设备上报以下信息至少之一:

网络的流量;

计费信息;

网络状态的监控信息;

网络能力的使用信息;

第二设备状态的监控信息。

52、一种通信装置，设置在第一设备上，包括:

处理单元，配置为为 UPF 发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。

53、一种第一设备，包括: 处理器及通信接口; 其中，

所述处理器，配置为为 UPF 发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能。

54、一种第一设备，包括: 处理器及和配置为存储能够在处理器上

运行的计算机程序的存储器，

其中，所述处理器配置为运行所述计算机程序时，执行权利要求 29 至 51 任一项所述方法的步骤。

55、一种存储介质，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权利要求 29 至 51 任一项所述方法的步骤。

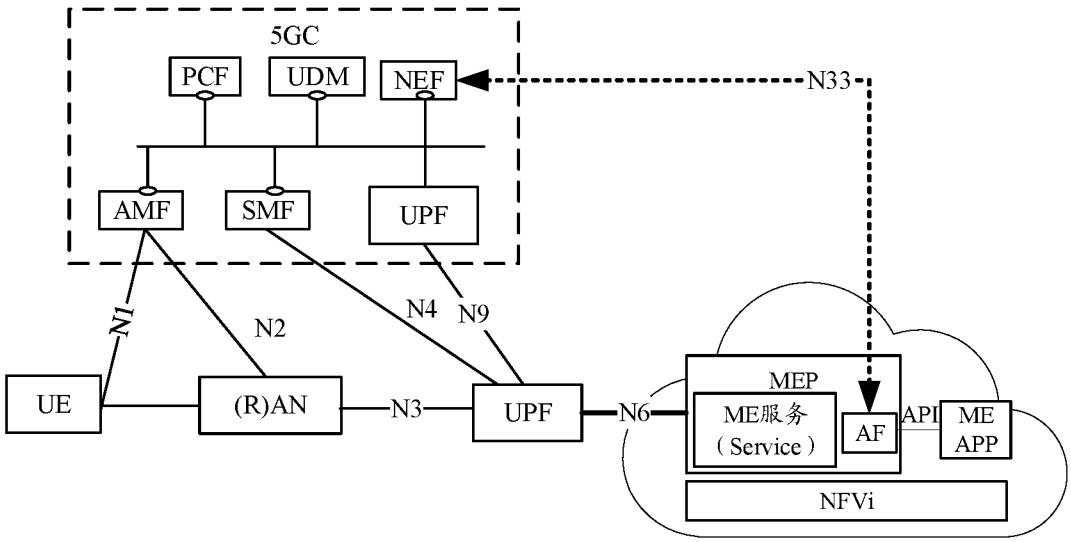
5GC
PCF
UDM
NEF
N33
AMF
SMF
UPF
N1
N2
N4
N9
UE
(R)AN
N3
UPF
N6
MEP
ME服务
（Service）
AF
API
ME
APP
NFVi

图 1

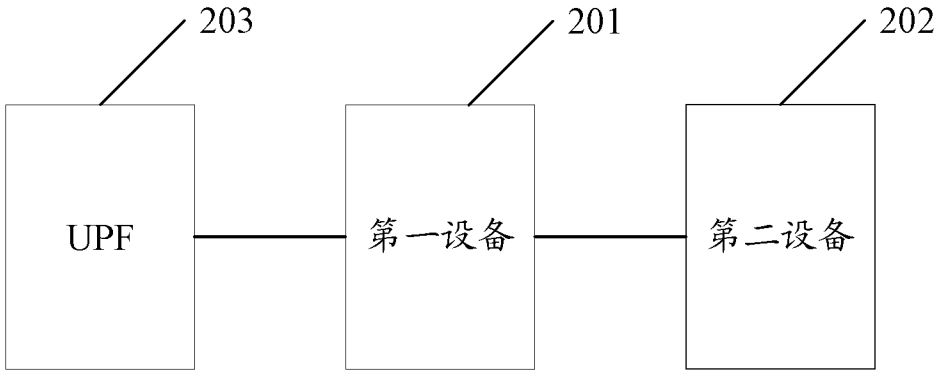
203
201
202
UPF
第一设备
第二设备

图 2

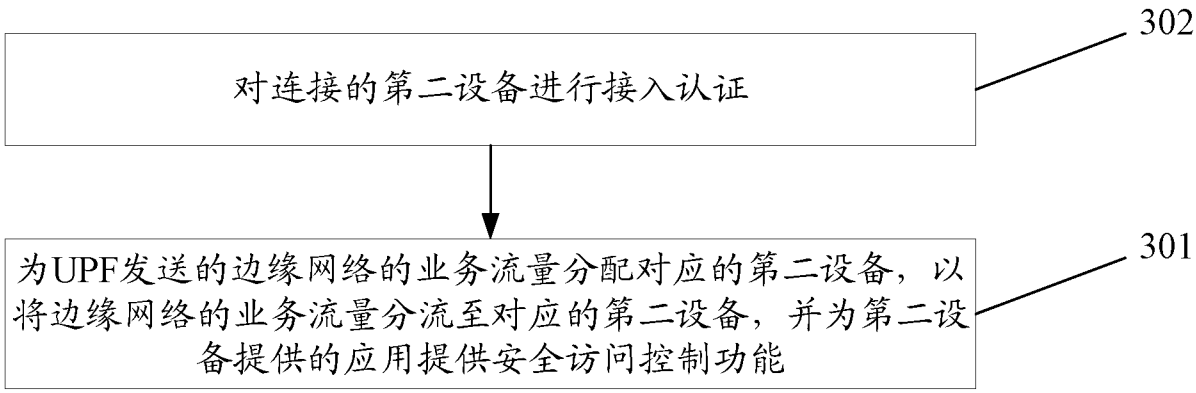
302
对连接的第二设备进行接入认证
301
为UPF发送的边缘网络的业务流量分配对应的第二设备，以将边缘网络的业务流量分流至对应的第二设备，并为第二设备提供的应用提供安全访问控制功能

图 3

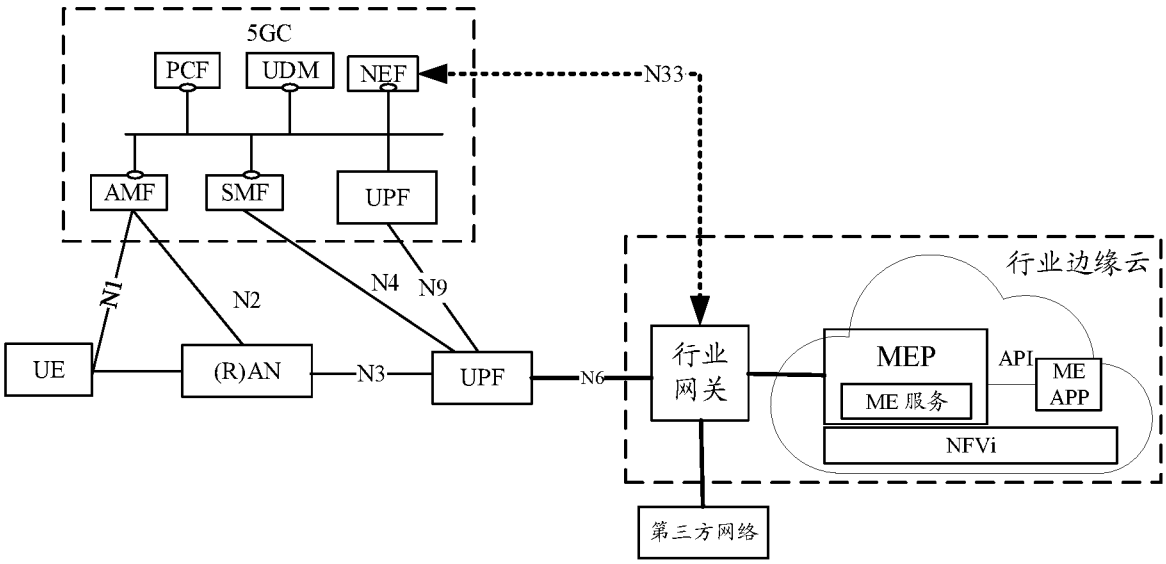
5GC
PCF
UDM
NEF
N33
AMF
SMF
UPF
行业边缘云
N1
N2
N4
N9
行业
网关
MEP
API
ME
APP
UE
(R)AN
N3
UPF
N6
ME 服务
NFVi
第三方网络

图 4

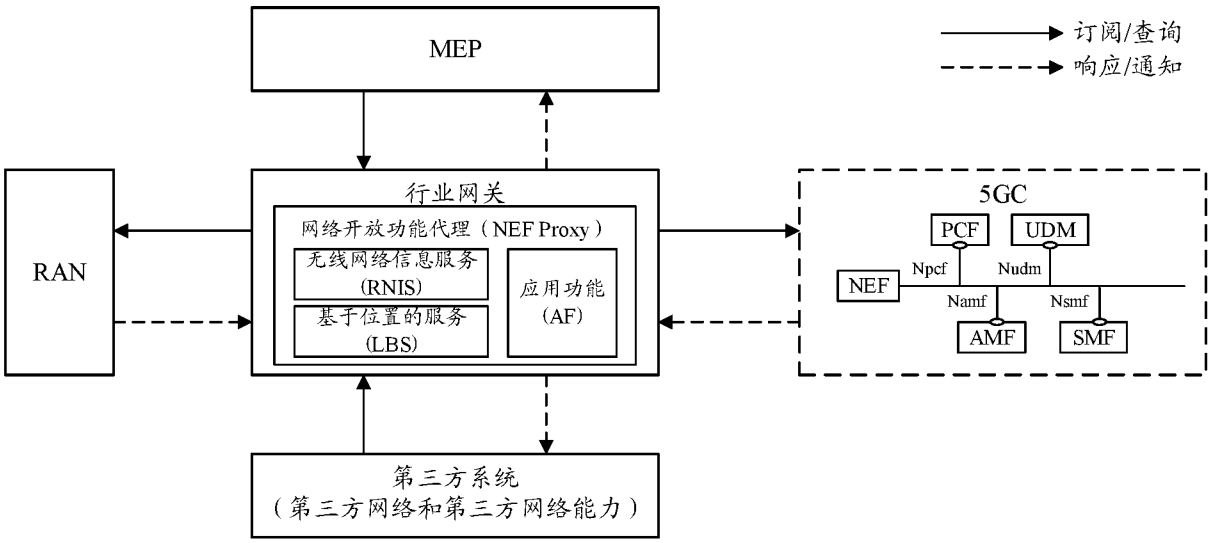
MEP
订阅/查询
响应/通知
行业网关
网络开放功能代理（NEF Proxy）
无线网络信息服务
(RNIS)
应用功能
(AF)
基于位置的服务
(LBS)
RAN
5GC
PCF
UDM
NEF
Npcf
Nudm
Namf
Nsmf
AMF
SMF
第三方系统
（第三方网络和第三方网络能力）

图 5

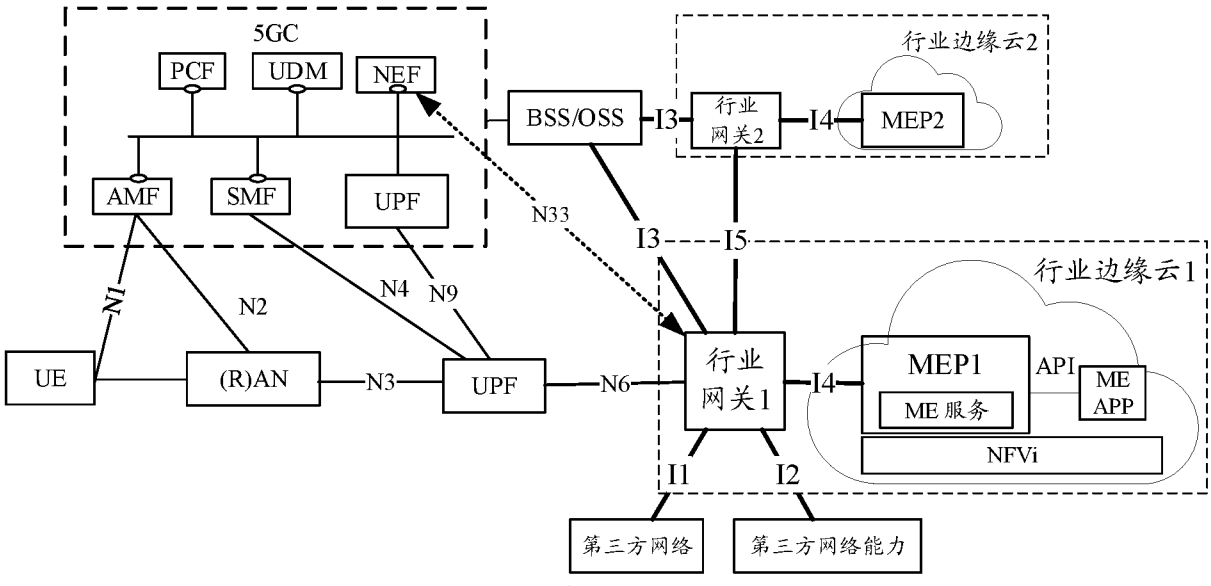
5GC
PCF
UDM
NEF
行业边缘云2
BSS/OSS
I3
行业
网关2
I4
MEP2
AMF
SMF
UPF
N33
I3
I5
行业边缘云1
N1
N2
N4
N9
UE
(R)AN
N3
UPF
N6
行业
网关1
I4
MEP1
API
ME
APP
ME 服务
NFVi
I1
I2
第三方网络
第三方网络能力

图 6

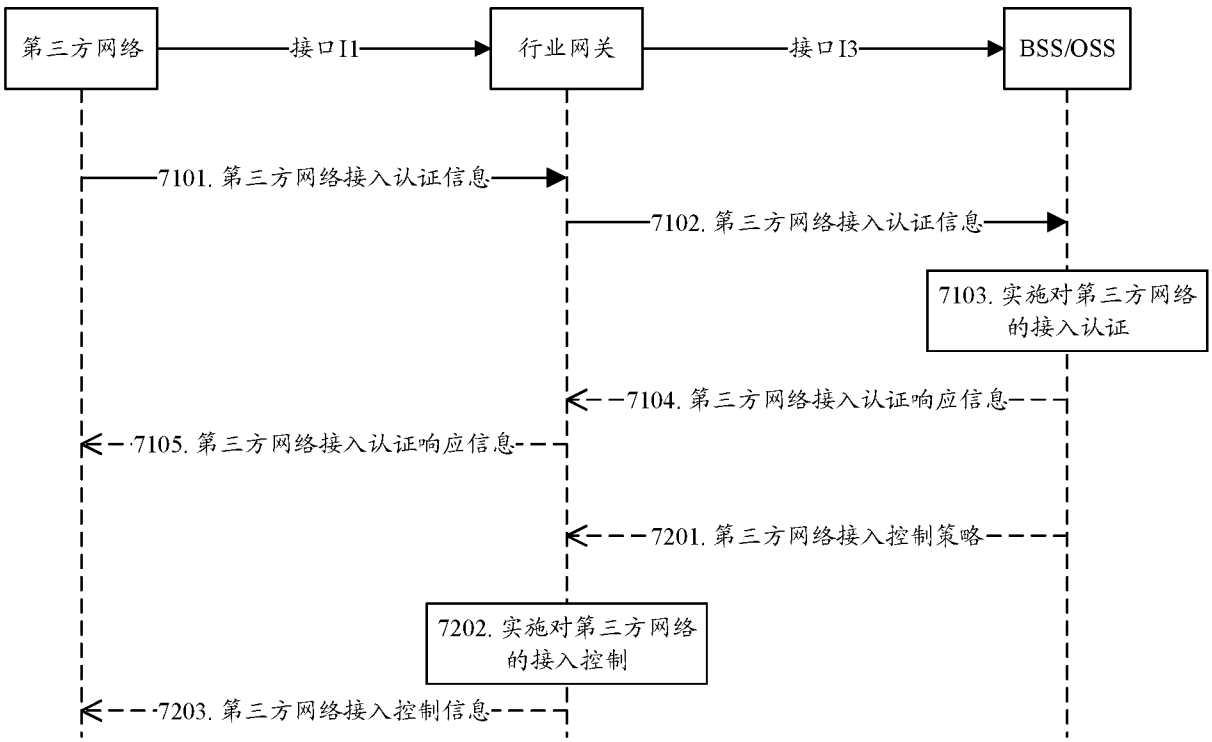
第三方网络
接口I1
行业网关
接口I3
BSS/OSS
7101. 第三方网络接入认证信息
7102. 第三方网络接入认证信息
7103. 实施对第三方网络的接入认证
7104. 第三方网络接入认证响应信息
7105. 第三方网络接入认证响应信息
7201. 第三方网络接入控制策略
7202. 实施对第三方网络的接入控制
7203. 第三方网络接入控制信息

图 7

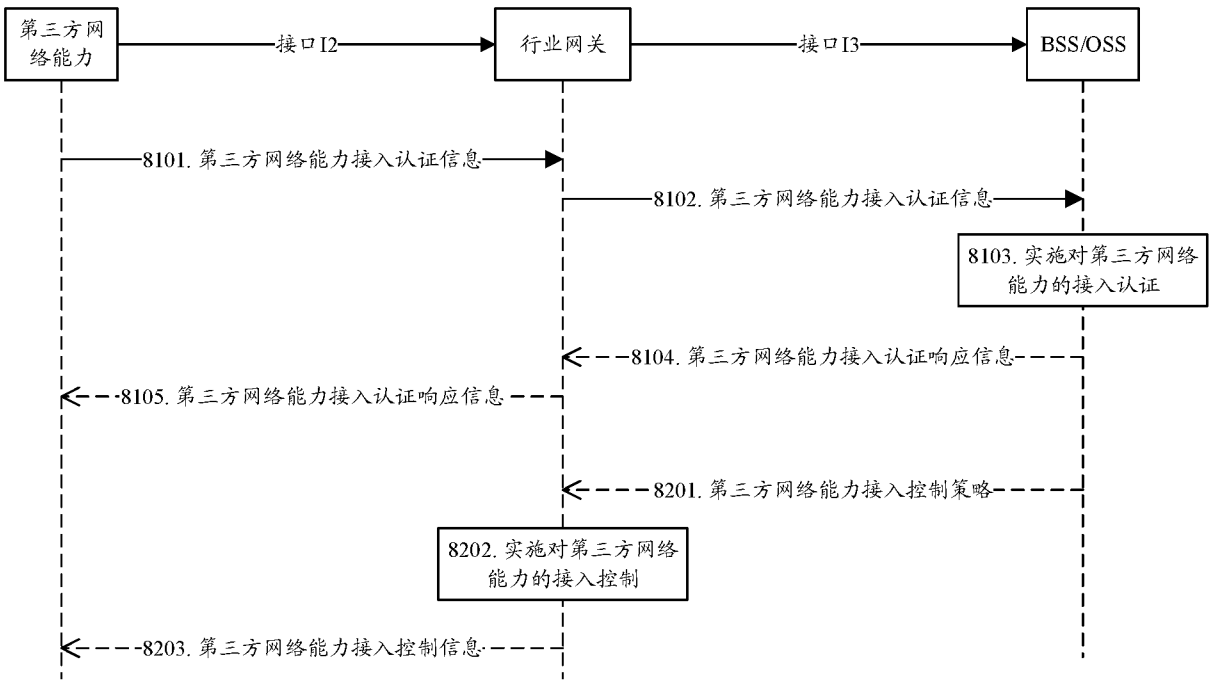
第三方网络能力
接口I2
行业网关
接口I3
BSS/OSS
8101. 第三方网络能力接入认证信息
8102. 第三方网络能力接入认证信息
8103. 实施对第三方网络能力的接入认证
8104. 第三方网络能力接入认证响应信息
8105. 第三方网络能力接入认证响应信息
8201. 第三方网络能力接入控制策略
8202. 实施对第三方网络能力的接入控制
8203. 第三方网络能力接入控制信息

图 8

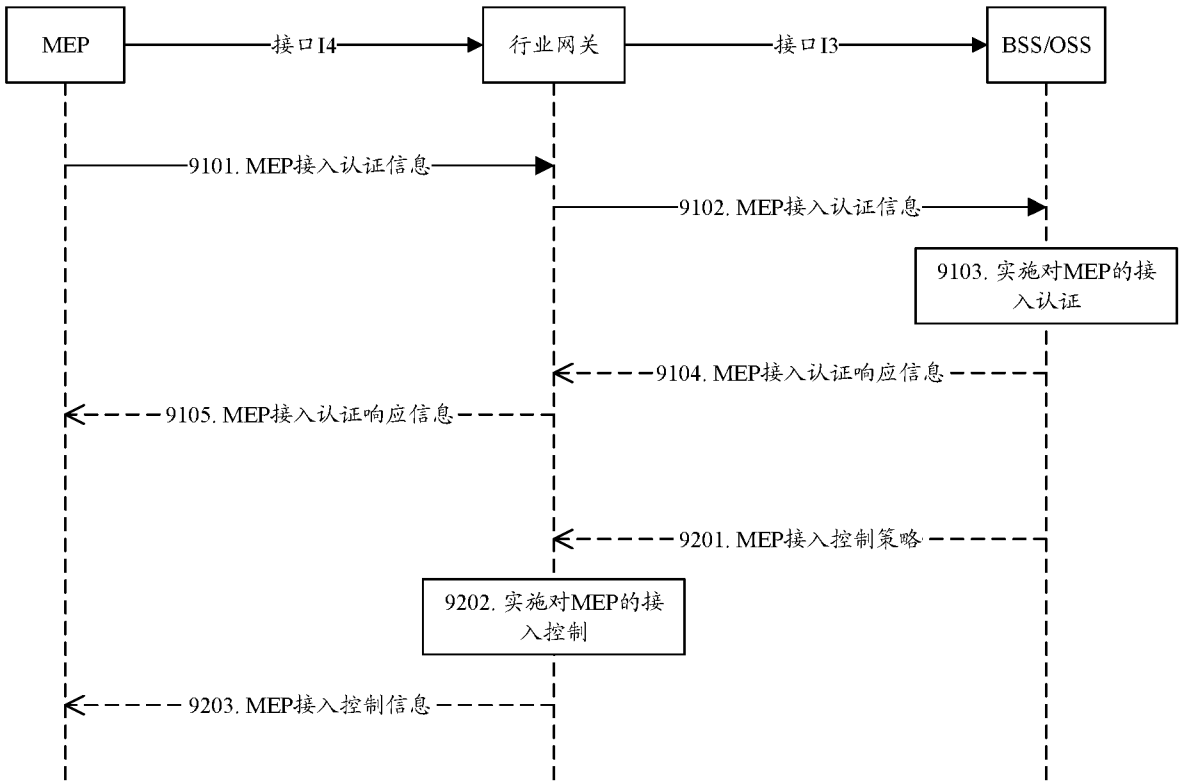
MEP
接口I4
行业网关
接口I3
BSS/OSS
9101. MEP接入认证信息
9102. MEP接入认证信息
9103. 实施对MEP的接入认证
9104. MEP接入认证响应信息
9105. MEP接入认证响应信息
9201. MEP接入控制策略
9202. 实施对MEP的接入控制
9203. MEP接入控制信息

图 9

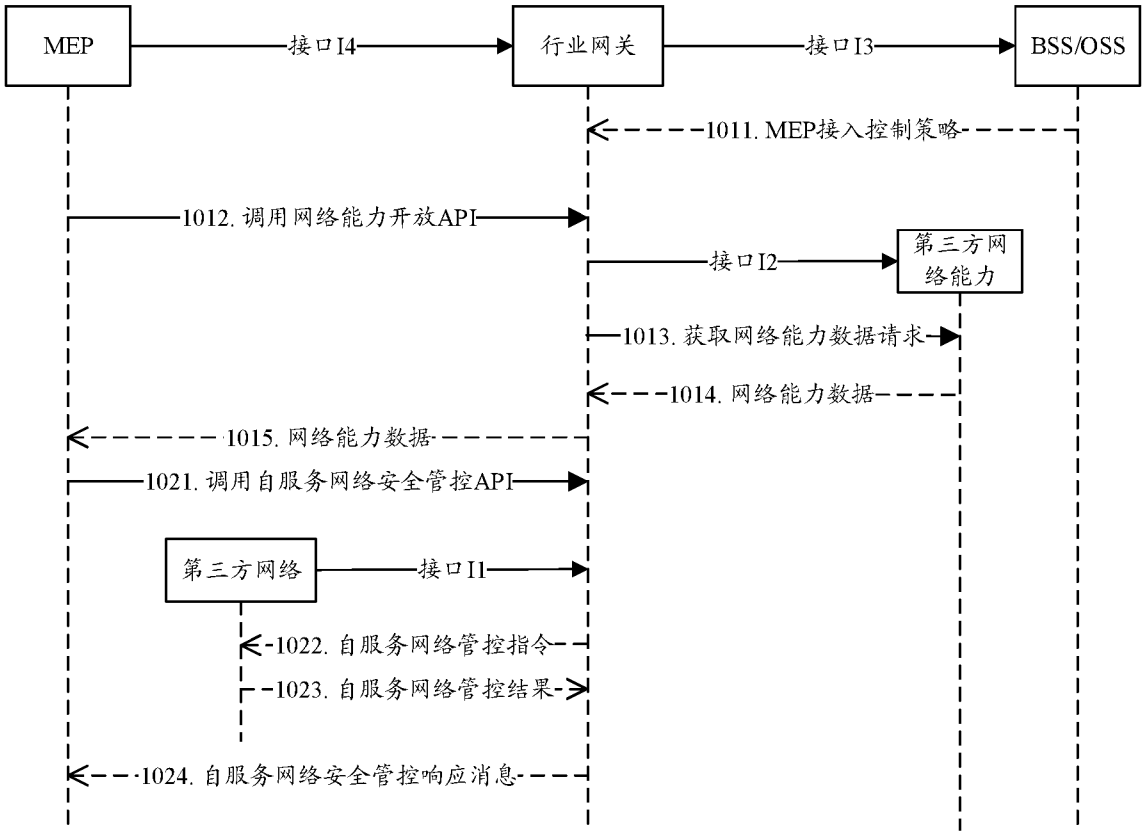
MEP
接口I4
行业网关
接口I3
BSS/OSS
1011. MEP接入控制策略
1012. 调用网络能力开放API
接口I2
第三方网络能力
1013. 获取网络能力数据请求
1014. 网络能力数据
1015. 网络能力数据
1021. 调用自服务网络安全管控API
第三方网络
接口I1
1022. 自服务网络管控指令
1023. 自服务网络管控结果
1024. 自服务网络安全管控响应消息

图 10

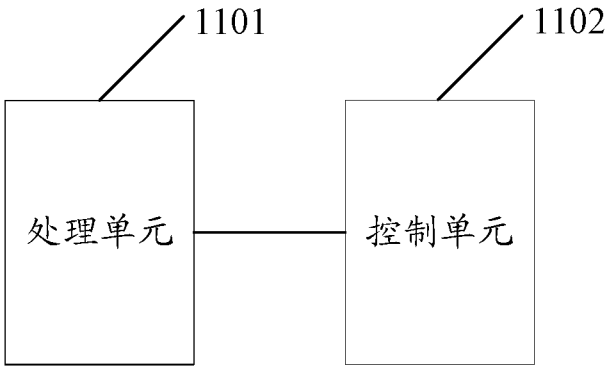
1101
1102
处理单元
控制单元

图 11

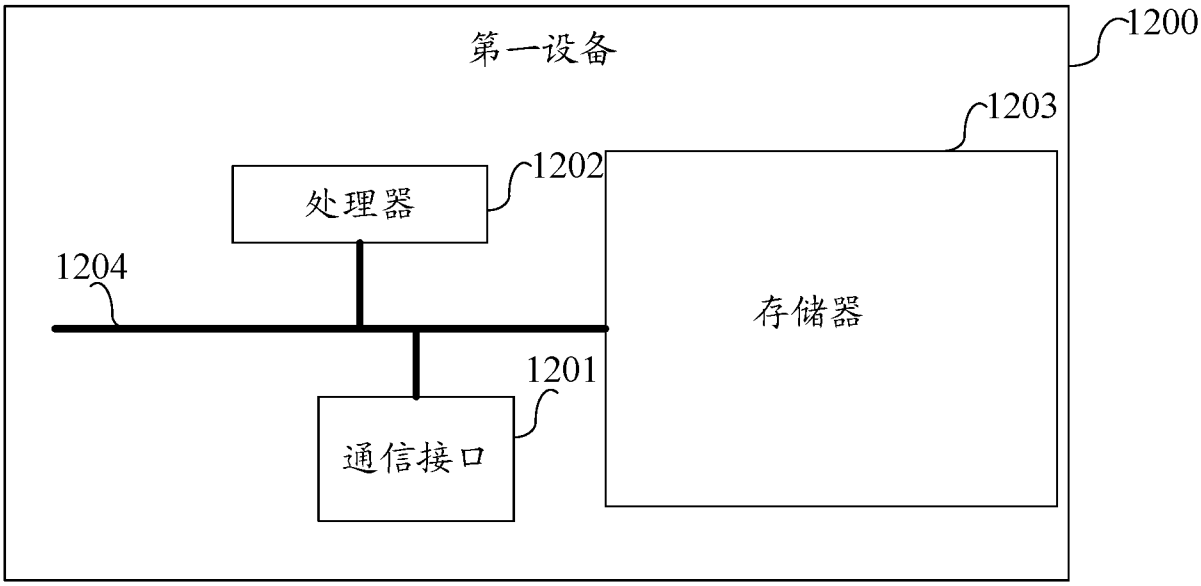
第一设备
1200
1203
处理器
1202
1204
存储器
1201
通信接口

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/100809

A. CLASSIFICATION OF SUBJECT MATTER

H04W 28/08(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)

H04W; H04L

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)

CNTXT; ENTXT; CNKI; WPABS; 3GPP: 用户平面功能, 用户面功能, 多接入边缘计算, 网关, 分配, 安全访问, 平台, 服务器, UPF, user plane function, MEC, multi-access edge computing, MEP, MEC plane, network gate, allocat+, distribut+, secur+, access, plane, server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 110198363 A (SHENZHEN TENCENT COMPUTER SYSTEMS CO., LTD.) 03 September 2019 (2019-09-03) description, paragraphs 5-10	1-55
Y	CN 105100109 A (HUAWEI TECHNOLOGIES CO., LTD.) 25 November 2015 (2015-11-25) description, paragraphs 5-10	1-55
A	CN 111787069 A (CHINA MOBILE XIONG'AN INFORMATION COMMUNICATION TECHNOLOGY CO., LTD.) 16 October 2020 (2020-10-16) entire document	1-55
A	CN 111083737 A (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.) 28 April 2020 (2020-04-28) entire document	1-55
A	CN 109889586 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 14 June 2019 (2019-06-14) entire document	1-55
A	US 2020120446 A1 (CISCO TECHNOLOGY, INC.) 16 April 2020 (2020-04-16) entire document	1-55

☐ 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
"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
18 August 2022	**02 September 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/100809

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110198363	A	03 September 2019	JP	2022522368	A	18 April 2022
				US	2021352042	A1	11 November 2021
				EP	3968610	A1	16 March 2022
				WO	2020228505	A1	19 November 2020
CN	105100109	A	25 November 2015	WO	2017028513	A1	23 February 2017
				US	2018191682	A1	05 July 2018
CN	111787069	A	16 October 2020		None		
CN	111083737	A	28 April 2020		None		
CN	109889586	A	14 June 2019		None		
US	2020120446	A1	16 April 2020	WO	2020081310	A1	23 April 2020
				EP	3868134	A1	25 August 2021
				US	2020280822	A1	03 September 2020

国际检索报告

国际申请号
PCT/CN2022/100809

A. 主题的分类

H04W 28/08(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)

H04W; H04L

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））

CNTXT;ENTXT;CNKI;WPABS;3GPP:用户平面功能，用户面功能，多接入边缘计算，网关，分配，安全访问，平台，服务器， UPF，user plane function, MEC，multi-access edge computing, MEP， MEC plane, network gate, allocat+, distribut+, secur+, access, plane, server

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 110198363 A (深圳市腾讯计算机系统有限公司) 2019年9月3日 (2019-09-03) 说明书第5-10段	1-55
Y	CN 105100109 A (华为技术有限公司) 2015年11月25日 (2015-11-25) 说明书第5-10段	1-55
A	CN 111787069 A (中移雄安信息通信科技有限公司等) 2020年10月16日 (2020-10-16) 全文	1-55
A	CN 111083737 A (大唐移动通信设备有限公司) 2020年4月28日 (2020-04-28) 全文	1-55
A	CN 109889586 A (腾讯科技深圳有限公司) 2019年6月14日 (2019-06-14) 全文	1-55
A	US 2020120446 A1 (CISCO TECH INC.) 2020年4月16日 (2020-04-16) 全文	1-55

☐ 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

“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
2022年8月18日	2022年9月2日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 毛韵楠 电话号码 86-(010)-62412160

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/100809

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	110198363	A	2019年9月3日	JP	2022522368	A	2022年4月18日
				US	2021352042	A1	2021年11月11日
				EP	3968610	A1	2022年3月16日
				WO	2020228505	A1	2020年11月19日
CN	105100109	A	2015年11月25日	WO	2017028513	A1	2017年2月23日
				US	2018191682	A1	2018年7月5日
CN	111787069	A	2020年10月16日		无		
CN	111083737	A	2020年4月28日		无		
CN	109889586	A	2019年6月14日		无		
US	2020120446	A1	2020年4月16日	WO	2020081310	A1	2020年4月23日
				EP	3868134	A1	2021年8月25日
				US	2020280822	A1	2020年9月3日