

TC609

全国数据标准化技术委员会技术文件

TC609-6-2026-XX

数据基础设施 高速数据流通网络技术要求

Data Infrastructure—Technical requirements for
high-speed data circulation network

（征求意见稿）

2026-XX-XX 发布

2026-XX-XX 实施

全国数据标准化技术委员会 发布

目 次

前 言	II
1 范围	3
2 规范性引用文件	3
3 术语和定义	3
4 缩略语	4
5 高速数据流通网络总体架构	4
5.1 定位与目标	4
5.2 高速数据流通网络架构	5
5.3 系统接口概述	6
5.4 高速数据流通网络接入场景概述	7
6 高速数据流通网络功能视图	7
6.1 概述	7
6.2 核心功能	8
7 接口交互关系	10
7.1 接口交互概述	10
7.2 网络服务接口	11
7.3 查询网络能力和状态	12
7.4 数据上报接口	12
8 高速数据流通网络部署方案	12
8.1 动态专网接入场景	12
8.2 静态接入场景	14
8.3 互联区	14
8.4 网络设施优化能力要求	15
8.5 互联网接入场景	15
附 录 A （资料性） 业务流程示例	18
附 录 B （资料性） 南北向交互接口参数	21
参 考 文 献	26

前 言

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国数据标准化技术委员会（SAC/TC609）提出并归口。

本文件起草单位：

数据基础设施 高速数据流通网络技术要求

1 范围

本文件规定了高速数据流通网络的总体架构和功能视图，规范了在数据高速流通过程中，数据基础设施与网络之间交互的技术要求。

本文件适用于各类型数据基础设施中数据流通网络的设计、建设和评价。支撑这些基础设施的技术体系包括但不限于数场、可信数据空间、数联网、数据元件、隐私保护计算、区块链等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

GB/T 43697-2024 数据安全技术 数据分类分级规则

3 术语和定义

下列术语和定义适用于本文件。

3.1

可信接入网关 Trusted Access Gateway

在企业或组织边界、数据通过其接入运营商网络的出口设备。

3.2

业务网关 Service Gateway

运营商接入数据流通专用网络（高速数据流通网互联区）的入口设备。

3.3

数联 PE Data Circulation Provider Edge

数据流通专用骨干网的边界路由器设备。

3.4

高速数据流通网络 Data Circulation Network

构建在现有网络基础设施之上，包含新增网元以及现有网络能力升级的数据流通业务专用网络。

3.5

应用感知网络策略标识 APN6 Identifier

基于用户身份标识、应用身份标识、数据对象标识等生成，封装在APN6扩展包头里，用于指向特定的网络质量保障、安全保障策略的字段。

3.6

随流可视 In-situ Observability

一种直接在业务数据报文中携带测量元数据的网络测量方法。

3.7

IPv6 段路由定位符 SRv6 Locator

一段全局路由可达的IPv6地址前缀，用于在网络中定位执行特定功能的SRv6节点及其关联的段标识（SID）。

4 缩略语

下列缩略语适用于本文件。

ACL：访问控制列表（Access Control List）

APN6：基于IPv6的应用感知网络（IPv6-based Application-aware Network）

BGP：边界网关协议（Border Gateway Protocol）

BGP RPD：边界网关协议-路由协议守护进程（BGP Routing Protocol Daemon）

EBGP：外部边界网关协议（External Border Gateway Protocol）

EDR：端点检测与响应（Endpoint Detection and Response）

IP：因特网协议（Internet Protocol）

IPv6：因特网协议第六版（Internet Protocol version 6）

IPSec6：基于IPv6的IP层安全机制（IPv6-based Internet Protocol Security）

IFIT：随流业务质量感知（In-situ Flow Information Telemetry）

PE：运营商边界（Provider Edge）

P：运营商（Provider）

QKD：量子密钥分发（Quantum Key Distribution）

SPA：单包授权（Single Packet Authorization）

SRv6：基于IPv6的分段路由（IPv6-based Segment Routing）

VPN：虚拟私有网络（Virtual Private Network）

5 高速数据流通网络总体架构

5.1 定位与目标

高速数据流通网络是支撑数据要素流通的网络底座，统一承载连接数据基础设施、算力设施、存储设施等，为数据基础设施提供数据高速流通服务。其基于传统网络设施升级改造，新增网元角色，并结合数据基础设施改造，使高速数据流通网络能够提供多方秒级灵活组网、弹性带宽、安全传输、路径可视可溯等能力，满足数据采集、汇聚、高速流通和全流程监管等业务需求。高速数据流通网络结合数据基础设施等，可支撑数场、可信数据空间、数联网、数据元件、隐私计算、区块链等多类技术体系应用落地。

高速数据流通网络在数据基础设施中的定位如下：

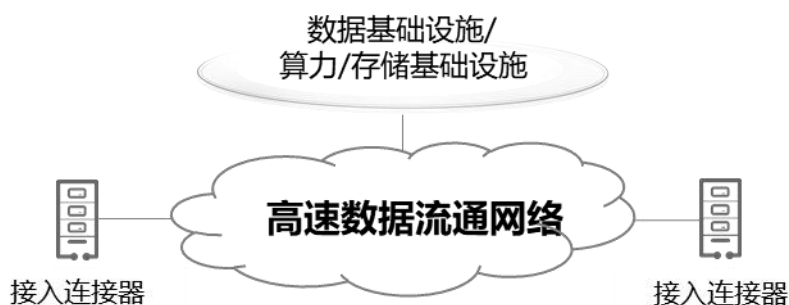


图 1 高速数据流通网络在数据基础设施中的定位

5.1.1 核心目标

高速数据流通网络的核心目标是针对数据流通业务，提供灵活调度、高质量、高安全、可溯源的数据传输服务，解决企业和机构通过互联网进行数据要素流通的可信问题，从而真正释放数据交易、数据共享的应用场景和价值。

5.2 高速数据流通网络架构

从组网的角度，高速数据流通网络模块架构如图2所示，包括网络模块和系统接口。

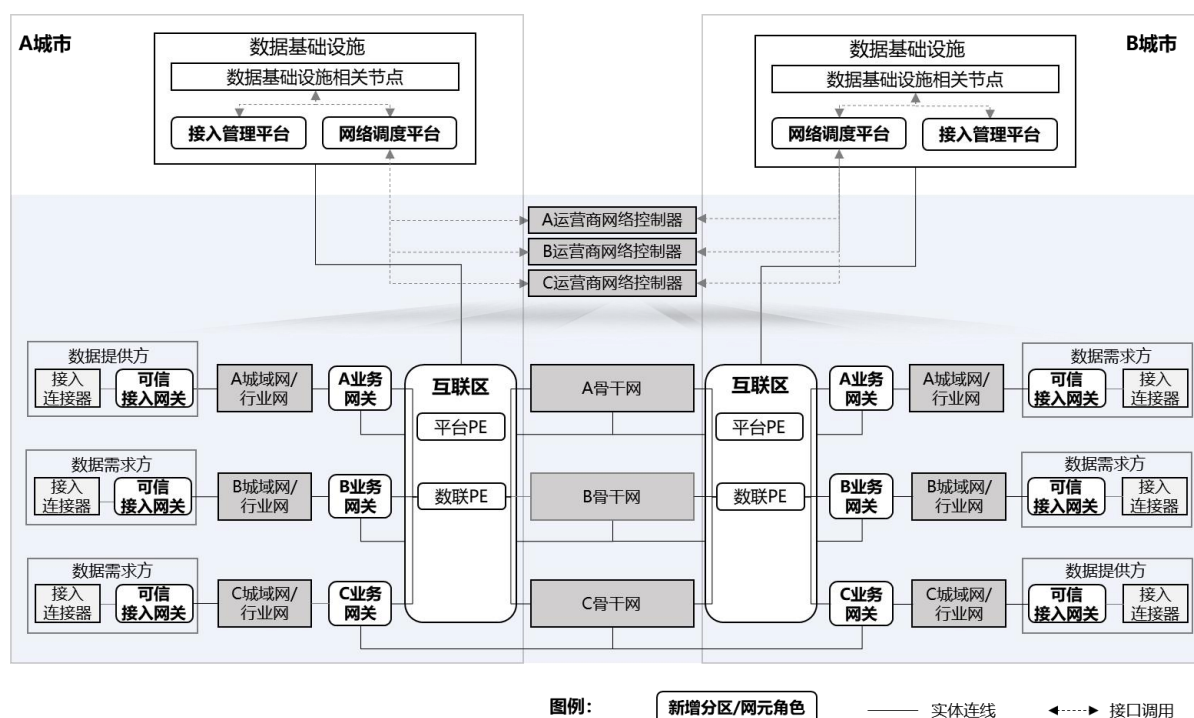


图 2 高速数据流通网络组网模块架构

主要新增以下关键网元或分区：

5.2.1 可信接入网关

可信接入网关作为企业或组织物理出口位置的网络接入实体，结合运营商城域网、行业专网，实现数据接入主体的接入连接器安全泛在地接入数据基础设施。可信接入网关通过SRv6协议形成灵活按需的连接，可信接入，同时完成数网标识映射和按需加密等。

5.2.2 业务网关

业务网关作为接入网络的业务策略控制网关，与可信接入网关配合，为数据接入主体提供快速建连、弹性带宽、传输安全等关键能力。业务网关和可信接入网关均由接入网络的责任主体管理（如对应城域网的运营商）。业务网关用于按需控制可信接入网关的组网连接，实现数据流通的弹性带宽控制、数据流通交易的隔离、传输加密和计费结算等。同时通过业务网关连接互联区，完成跨域跨网的策略控制。地市内每运营商/专网需部署至少一对业务网关。

5.2.3 互联区

互联区用于解决各类数据接入主体经由异构运营商网络/行业网络接入数据基础设施场景下，接入主体间的数据如何高速流通的问题。网络互联区对接各类运营商城域网/行业专网的业务网关，并提供数据接入主体间数据流通的安全隔离、跨网计费结算等功能。同时通过互联区统一对接数据基础设施，为数据基础设施按需调度网络服务提供管控通道。

数联PE是互联区的核心组件。各类接入网络的业务网关由数联PE完成对接。依托数联PE，提供异构网络的动态路由策略和转发策略控制，可实现跨网数据供需方之间的数据安全隔离，带宽弹性调度，跨网计费结算、跨网数据防泄露等流通保障能力。面向各运营商城域网和行业专网，互联区宜成对配置数联PE，便于运维管理与故障域隔离。

同时互联区宜增设至少一对平台PE，用于对接数据基础设施相关节点、网络调度平台、接入管理平台等数据基础设施及各类算力设施等；互联区内宜部署P节点，降低多台数联PE全互联的线路部署压力。

5.2.4 接入管理平台

在数据基础设施体系内，配套建设面向高速数据流通网络的接入管理平台。通过接入管理平台可完成数据接入主体的数据流通网络入网申请、接入权限全生命周期管控等工作。同时接入管理平台融合零信任接入访问等能力，联动零信任接入网关，支撑数据接入主体经由互联网安全接入并访问高速数据流通网络内一般数据的场景。

5.2.5 网络调度平台

在数据基础设施体系内，配套建设面向高速数据流通网络的网络调度平台。用于高速数据流通网络的服务管理与调度，并开放系统接口对接数据基础设施相关节点、重要功能设施及运营商网络控制器等。通过网络调度平台接收数据流通交易指令，并传递到对应的运营商网络控制器，快速实现数据接入主体间的安全高速流通的连接建立和调度。

5.3 系统接口概述

高速数据流通网络的系统接口以网络调度平台为中心，分为北向和南向两个接口域。每个接口域内均包含网络服务接口、状态同步接口和数据上报接口三类接口，每类接口由若干接口操作组成。接口域的划分、接口分类、接口操作列表要求见第7章。

5.3.1 面向数据基础设施相关节点的接口

该接口是网络调度平台面向数据基础设施相关节点的开放接口，该接口域整体呈双向交互结构：数据基础设施相关节点向网络调度平台进行连接调度、策略下发和状态查询，网络调度平台向数据基础设施相关节点反馈流通统计与日志信息：

- a) 下行：数据基础设施相关调度节点对网络调度平台进行连接调度和策略配置，主要内容为发放有数据流通/交易需求的接入连接器的标识信息，明确接入连接器之间按需灵活组网的连接、带宽等需求，同时下发业务所需的传输安全等级、网络 SLA 保障等需求；
- b) 上行：网络调度平台上报数据流通网络的数据流通统计、日志统计等信息，以供上层业务的监管和溯源等功用。

5.3.2 面向运营商网络控制器的接口

该接口是网络调度平台与运营商网络控制器之间的对接接口，用于调用高速数据流通网络资源。该接口域同样包含网络调度平台下发策略到运营商网络控制器，以及运营商网络控制器上报统计信息两个方向：

- 下行：网络调度平台将获取的接入主体标识信息和安全高速需求转换为网络地址信息和网络控制策略，并通过该接口下发到运营商网络控制器，运营商网络控制器调度对应的接入网关，业务网关和城域网/骨干网设备，完成灵活组网和策略控制。
- 上行：运营商网络控制器获取连接状态信息，数据流通质量统计，流路径存证，计费计量等信息，上送网络调度平台，供上层业务按需调度。

5.4 高速数据流通网络接入场景概述

高速数据流通网络主要包含静态专线接入、动态专网接入两类主流接入场景，可支撑一般数据、重要数据的流通传输。

- 动态专网接入场景：由运营商或行业专网提供数联专网服务，满足企业间动态按需组网、快速建连、跨网灵活对接、弹性带宽调整等动态弹性业务需求。
- 静态专线场景：由运营商提供独立的物理隔离的专线资源接入互联区，由互联区统一完成与各类网络资源下接入连接器的互通与调度。
- 对于互联网接入，可依托接入管理平台与零信任网关，实现与高速数据流通网络各类接入场景的互联互通，主要承载 API 接口数据、普通数据集等保密要求较低的数据，高效满足常态化、轻量化的数据流通需求。

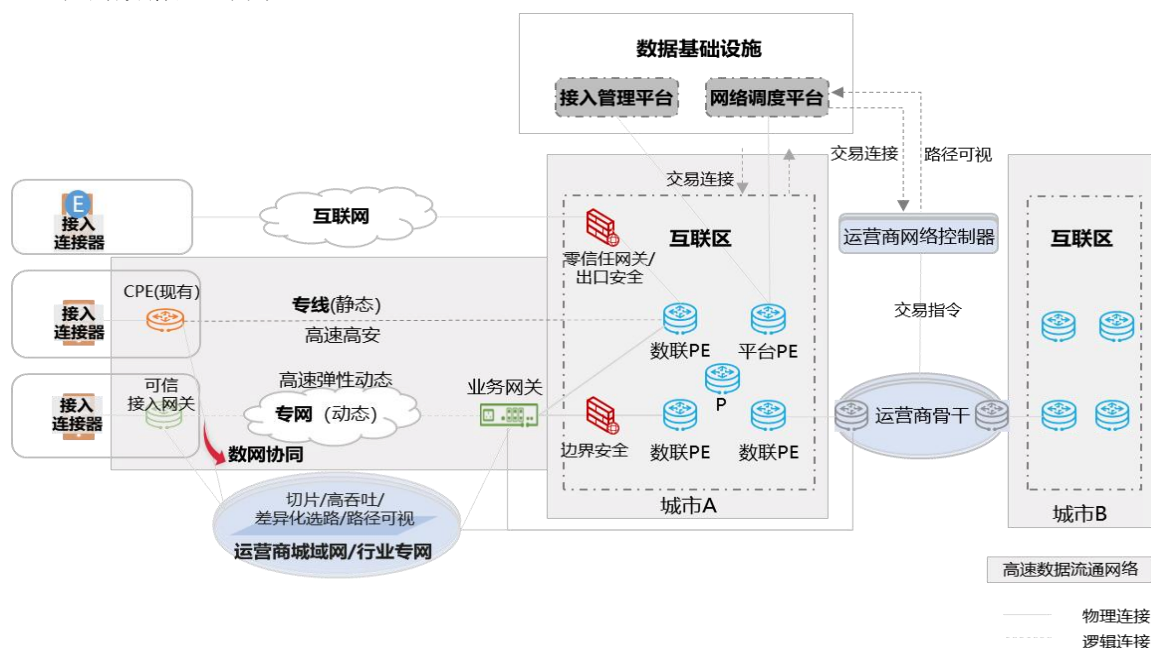


图 3 高速数据流通网络场景视图

6 高速数据流通网络功能视图

6.1 概述

高速数据流通网络功能视图包含高速数据流通网接入网元（可信接入网关+业务网关），高速数据流通网络互联区和网络调度平台/接入管理平台等关键角色。三层架构间配合，共同提供高速数据流通网络关键能力。



图 4 高速数据流通网络功能视图

6.2 核心功能

6.2.1 灵活组网（控制面）

由网络互联区+可信接入网关+业务网关+网络调度平台配合实现。高速数据流通网应能够基于数据供需方交易流通需求，配合控制面秒级建连策略，按需建立VPN连接，并秒级建立IPv6+隧道。

企业出口可信接入网关，业务网关和互联区数联PE均应支持IPv6+动态连接。默认接入数据流通网络的企业之间都无法互联且无对应路由，网络调度平台通过数据基础设施相关调度节点获取供需方的连接标识信息，业务网关兼做RR，通过路由策略控制实现基于交易的秒级的按需连接。

接入连接器应支持IPv6地址，通过IPv6的海量地址，确保接入连接器之间按需互通且地址不冲突。

6.2.2 交易隔离（转发面）

依托网络互联区、可信接入网关、业务网关协同联动实现高速数据流通网络的交易级隔离。

业务网关/数联PE应基于数据供需方交易流通需求，通过转发面精细化的会话隔离策略，实现交易级安全隔离，确保数据要素流通安全。

6.2.3 网络标识

可信接入网关、业务网关和互联区应支持网络标识能力，基于IPv6+的数据与网络协同标识技术（如基于APN6, ARN, SAN等实现），在数据流通报文中应由接入连接器或可信接入网关基于数据分级分类和关键需求完成标识的写入，应确保网络能正确解析数据类型并完成安全、选路等策略控制。APN6标识宜具备防篡改和标识隐藏的能力。可信接入网关，业务网关均应支持网络标识，网络基础设施、网络互联区应支持基于数据和网络标识的映射，提供差异化保障。

6.2.4 弹性带宽

网络互联区，业务网关，可信接入网关配合现有网络基础设施，基于数据传输需求定制传输任务、传输时间，实现网络和带宽资源快速调整，提高数据传输效率。

可信接入网关/业务网关/数联PE应支持基于连接的弹性带宽；网络基础设施应提供独立的数据流通资源保障，提供大颗粒面向数联服务的物理隔离的切片保障或小颗粒面向关键数据/关键接入主体的物理隔离切片保障，并能够根据传输需求动态调整切片资源。

6.2.5 路径可视/可视溯源

依托高速数据流通网和网络基础设施部署随流可视技术，逐跳记录数据流通过路信息，在可信接入网关、传统网络基础设施、业务网关和互联区提供全流程路径和策略执行的可视和审计能力。网络调度平台应根据数据标识等信息进行端到端路径拼接，提供关键数据的路径可视呈现和存证，支撑流通可追溯或异常溯源。

6.2.6 计量计费

业务网关、网络互联区和网络调度平台应结合交易级隔离策略，配合实现域内/跨域/跨网交易级流量计费计量、话单处理能力，包括生成、汇总、上报、稽核。将跨域交易数据转化为可稽核、可对账的标准化话单。满足跨运营商业务结算对账、精准核算的运营需求。

6.2.7 超高吞吐

网络互联区、网络基础设施应提供满足高质量数据集高吞吐承载，可基于流级负载均衡，深度hash等技术实现带宽充分利用，提升带宽利用率。

6.2.8 差异化保障

传统网络基础设施应根据数据分级分类的不同需求提供不同服务，基于网络标识，如APN6标识等，为高安全数据提供切片隔离和可信路径、为有高吞吐需求的高质量数据集提供带宽保障或通过负载均衡满足带宽需求、为实时数据提供低时延路径。

6.2.9 零信任接入

面向API接口数据、一般数据集等保密诉求较低的数据，可以通过互联网专线+零信任接入等权限和安全策略控制后，与通过高速数据流通网接入的接入连接器互通。零信任接入主要由支持零信任代理的零信任网关提供，接入网关需逐包查验权限，通过最小权限授权获取信息。接入连接器可通过安装EDR或内置SPA认证等能力配合零信任接入。关键能力包含：

- a) 零信任接入代理：零信任网关通过接入管理平台获取用户权限，逐包查验权限，通过最小权限授权获取信息。
- b) 资产隐藏：接入连接器在互联网场景隐藏原始地址，通过数据流通网互联区 IP（虚拟 IP）提供服务。零信任网关应提供虚拟 IP 代理。从而实现接入连接器资产隐藏。其他企业用户不会通过互联网直接访问到接入连接器，而是访问虚拟 IP，通过零信任代理网关跳转到接入连接器；
- c) 零信任接入策略：应对接业务节点，基于数据流通交易撮合，在互联网场景下获取用户互访权限和可信资产列表，并将策略协同到各运营商的零信任代理控制器；

6.2.10 安全保障能力

高速数据流通网需提供边界安全，传输加密等安全增强能力，确保数据流通安全。

- a) 边界安全：需在分域边界部署边界安全能力。包含企业与网络之间（可信接入网关），网络互联区与异构网络之间，互联网与高速数据流通网之间，应部署边界安全能力，包含防火墙、入侵检测、防病毒等能力，以应对企业之间数据流通的安全威胁。

- b) 流通安全：高速数据流通网和网络基础设施应具备数据流通防泄露等能力，如防镜像检测、防分光检测等，避免数据在流通过程中被窃取。
- c) 传输加密：数据流通中宜通过加密技术（如 IPSec 传输模式加密等）确保信息不泄露，可结合硬件加速能力，实现高性能的加解密，引入时延宜小于 1 毫秒。可按需叠加量子加密等方式，应对量子攻击。可信接入网关和业务网关宜支持传输加密。

7 接口交互关系

7.1 接口交互概述

高速数据流通网络需提供网络服务接口和数据上报接口等接口，满足数据基础设施对网络的服务调用等需求。高速数据流通网络的接口交互以网络调度平台为中心，划分为北向、南向两个接口域。北向接口命名为网络服务接口，南向接口命名为网络资源调度接口。

- a) 网络服务节点：数据基础设施相关节点与网络调度平台之间的接口域，承载数据流通业务侧发起的网络服务申请、状态查询以及网络侧向业务侧的运行信息上报；
- b) 网络资源调度接口：网络调度平台与运营商网络控制器之间的接口域，承载网络调度平台向网络侧下发的能力开通、策略配置指令以及网络侧向调度平台的运行信息上报。

网络调度平台负责两个接口域之间的转换与汇聚，将数据基础设施侧的接入连接器标识、合约标识等业务标识转换为运营商网络端点IP节点和网络控制策略后下发至运营商网络控制器；将运营商网络控制器反馈的网络信息汇聚后回传至数据基础设施相关节点。接口交互总体架构见图5。

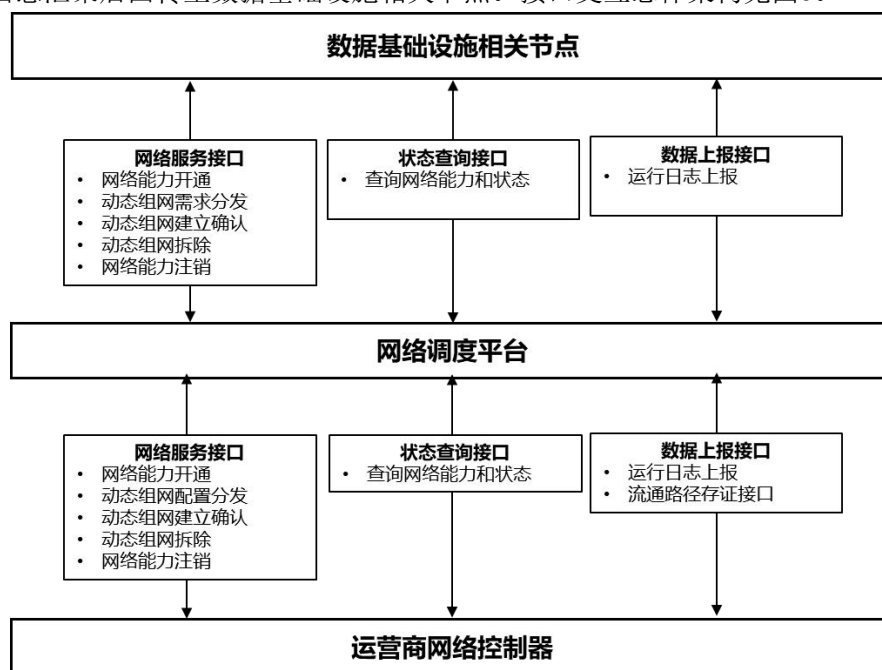


图 5 高速数据流通网络服务调用接口业务流程示意图

两个接口域内的接口按功能分为网络服务接口、状态查询接口和数据上报接口三类。每类接口由若干接口操作组成，接口操作是接口调用的最小单元，具有独立的接口操作编码、调用方、提供方以及请求参数和响应参数等。三类接口的功能定位如下：

- a) 网络服务接口：由网络能力开通、网络能力拆除、动态组网需求分发，建立确认和拆除等接口操作组成，用于网络能力的开通确认、网络服务的调用，是数据基础设施驱动网络的主通道；

- b) 状态查询接口：主用于查询接入连接器对应的网络能力、网络接入状态、连接状态等，为数据流通业务的组网可行性判断；
- c) 数据上报接口：由运行日志上报和流通过程存证上报等接口操作组成，用于运行信息的上报，支撑数据流通全过程的可视、可监控和可溯源。

各类接口操作的参数参见附录 B。

7.2 网络服务接口网络能力开通

该接口操作用于运营商控制器向网络调度平台，以及网络调度平台向数据基础设施相关节点同步接入连接器对应的高速数据流通网络能力开通情况，业务流程见附录A. 1。

以接入连接器标识为关联对象，实现接入连接器与高速数据流通网络之间的接入关系建立同步。

关键参数包含：接入连接器标识ID，网络提供方ID，接入类型，可支持的最大带宽等。

7.2.2 网络能力注销

该接口操作用于运营商控制器向网络调度平台，以及网络调度平台向数据基础设施相关节点同步网络能力注销情况，业务流程见附录A. 2。

以接入连接器标识为关联对象，实现接入连接器与高速数据流通网络之间的接入关系解除同步。

关键参数包含：接入连接器标识ID，网络提供方ID等

7.2.3 动态组网需求分发

该接口操作用于数据基础设施相关节点在数据供需双方签订交易合约后，向网络调度平台下发组网需求，结合配置分发接口操作，建立数据供给方接入连接器与数据订购方接入连接器之间的连接，业务流程见附录A. 3。

关键参数包含：供需方接入连接器标识ID，合约ID，带宽，时延，保障等级等

7.2.4 动态组网配置分发

该接口操作用于网络调度平台将组网需求转换后的网络控制策略下发至运营商网络控制器，业务流程见附录A. 3。下发参数继承北向下发组网需求接口的参数，以合约标识、连接标识、数据供给方与数据提供方的接入连接器标识及服务质量参数进行描述，同时增加接入连接器地址等信息。运营商网络控制器应根据本侧角色，对其管辖的运营商网络端点完成路由策略发布、隧道建立、会话隔离策略配置和带宽保障配置，并按连接维度实施交易级隔离，确保不同连接之间的数据流互不可见。

关键参数包含：供需方接入连接器标识ID，合约ID，接入连接器IP地址，带宽，时延，保障等级等

7.2.5 动态组网建立确认

该接口操作用于运营商网络控制器在完成本侧网络服务配置后，向网络调度平台确认本侧动态连接的建立结果。网络调度平台汇总数据供需双方各侧的确认结果并完成连通性确认后，再通过北向动态连接建立确认接口向数据基础设施相关节点回传连接建立结果。业务流程见附录A. 3。

关键参数包含：供需方接入连接器标识ID，合约ID等。

7.2.6 动态组网拆除连接

该接口操作用于网络调度平台基于合约标识向运营商网络控制器下发连接拆除配置，业务流程见附录A. 4。运营商网络控制器应根据合约标识和本侧接入连接器地址，可信接入网关地址定位对应的连接，撤销相关路由策略、隧道和隔离策略，并释放带宽资源。网络调度平台应汇总数据供给方侧和数据需求

方侧的结果同步，各侧均拆除成功后，通过北向基于合约标识申请拆除连接接口操作的结果同步向数据基础设施相关节点回传连接状态为已拆除。

关键参数包含：供需方接入连接器标识ID，连接器IP地址，合约ID等。

7.3 查询网络能力和状态

状态查询接口用于在网络服务调用前查询高速数据流通网络的网络能力和运行状态。

该接口操作用于数据基础设施相关节点向网络调度平台，以及网络调度平台向相关运营商查询接入连接器的网络能力、网络接入状态、连接状态以及网络质量和流量信息等。

关键参数包含：接入连接器标识ID，网络提供方ID等

7.4 数据上报接口

数据上报接口涵盖运行日志上报、流通过程存证等服务。运营商网络控制器向网络调度平台上报运行状态，网络链路监控数据和数据流通过程等内容，支持周期定时上报与即时按需上报两种模式，上报内容涵盖接入运行状态、交付流通统计，流量路径可视等内容，支撑数据流通业务实现可视、可监控、可溯源。**运行日志上报**

用于运营商网络控制器向网络调度平台上报接入主体的运行状态日志，包括接入连接器在线/离线状态、网络链路连通状态、带宽利用率、异常告警等运行信息，支持周期定时上报与即时按需上报两种模式，为网络运行监控和故障诊断提供数据支撑。

7.4.2 流通过程存证接口

用于记录和存证数据流通过程中的网络传输路径信息。运营商网络控制器向网络调度平台上报数据流通的实际传输路径、经过的网络节点、时间戳等信息，在网络调度平台可实现数据流通全过程的路径可视化与可追溯，为数据流通合规审计、安全溯源和争议处理提供路径存证依据。

向网络调度平台上报数据流通的实际传输路径信息。上报内容宜包含：

- a) 路径信息：数据流通实际经过的网络节点序列、各节点的进出时间戳；
- b) 关联信息：连接标识、合约标识以及数据供需双方的运营商可信接入网关 IP 地址；
- c) 策略信息：路径上执行的策略标识，交易流统计，隔离策略及其执行结果等

8 高速数据流通网络部署方案

8.1 动态专网接入场景

8.1.1 网络部署方案

数据供需方通过动态专网接入，基于交易需求灵活组网是高速数据流通网的主要组成场景。

数据供需方通过该接入方式接入后，数据流通关系包含网内，跨网，跨域等多个子场景。

- a) 网内互联：通过可信接入网关+业务网关+运营商城域网数联专网/行业专网组成；
- b) 跨网互联：由网内互联子场景+互联区组成
- c) 跨域互联：分为两类场景：1) 单运营商内跨地市，由网内互联子场景+运营商骨干网；2) 跨运营商跨地市，在单运营商跨域基础上增加互联区。

本节主要介绍网内互联场景，跨网跨域场景需结合互联区方案部署。

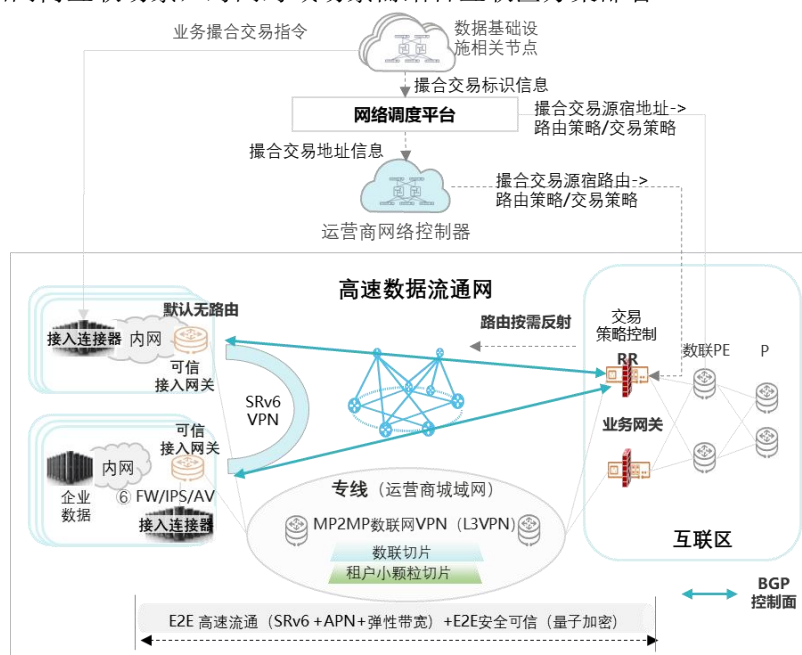


图 7 高速数据流通网络动态接入场景方案图示

动态专网接入场景部署采用可信接入网关和业务网关之间构建SRv6隧道承载数据流通业务，依托SRv6隧道实现跨运营商网络/行业专网的穿通传输，由运营商为可信接入网关和业务网关分配全网唯一的SRv6 Locator，并在运营商网络通过三层VPN（数联网VPN）完成可信接入网关与专线业务网关间SRv6 Locator路由的互通传递。确保数据流通业务在网络传递中与其他业务隔离。

通过动态专网接入的数据主体间，接入连接器之间默认不可连通，企业可信接入网关仅有本地业务路由，以及业务节点运营商控制器等平台路由。在可信接入网关间有通信需求时，通过BGP扩展协议等方式动态部署路由策略，基于流通交易按需发布企业接入网关之间的业务路由，实现企业间业务通信。同时业务网关基于交易信息形成转发面交易隔离，完成认证鉴权和计费。

可信接入网关之间、业务网关与可信接入网关之间支持宜对传输数据进行加密，加密算法支持国家密码局密码要求，宜支持量子加密。

8.1.2 关键角色能力要求可信接入网关能力要求

作为高速数据流通网络在接入连接器侧的连接实体，部署于企业局域网出口，通过可信接入网关实现企业/行业接入连接器的高效、安全接入高速数据网，并对高速数据网进行边界安全防护。

可信接入网关具备以下要求：

- 应支持SRv6、随流检测（如IFIT等）能力；
- 应支持基于IPv6+的灵活组网和基于交易的快速建删能力，建连时间≤1秒；
- 应支持弹性带宽能力，满足不同规模数据资源传输，弹性带宽范围宜满足100M-10G；
- 应支持基于IPv6+的数网协同能力，如APN6等，支持数据分级分类与网络标识映射。
- 宜支持访问控制、包过滤、IPS、AV等边界安全能力；
- 宜支持IPsec、Xsec、MACsec等加密协议，宜支持量子加密，支持国密算法等；

● 业务网关能力要求

作为接入网络与互联区的连接实体，部署于互联区）的边缘，连接枢纽数联PE。与可信接入网关相互配合实现企业/行业接入连接器的按需高速连接、弹性带宽分配和数据传输加密，并实现对数据流通过程的可视存证，交易级隔离和计费以及可视溯源。

专线业务网关具备以下能力：

- a) 应支持基于 IPv6+的灵活组网和基于交易的路由策略能力，建连时间 ≤ 1 秒；
- b) 应支持交易级访问策略控制和会话隔离，确保数据流通安全和隔离；
- c) 应支持 SRv6、随流检测（如 IFIT 等）等技术能力；
- d) 宜支持基于 IPv6+的网络标识映射能力，支持数据分级分类与网络标识映射。
- e) 宜支持 IPsec、xSec、MACsec 等传输加密协议，宜支持量子加密，国密算法、PQC 算法等；

● 接入连接器能力依赖

接入连接器应支持IPv6地址接入高速数据网，确保地址不冲突。静态接入场景能力要求同。

8.2 静态接入场景

8.2.1 网络部署方案

静态专线接入场景采用固定接入模式，依托运营商二层专线直连网络互联区，由互联区的运营主体统一提供静态的数据流通服务，具备高稳定、高安全性的网络互联能力。各接入主体独享物理接口资源，并通过逻辑VPN实现业务隔离。

具备互通需求的静态专线接入主体，经由 VPN 路由交叉调度，可实现跨网络、跨地市的数据安全高速流转；支持数据供需双方多点到多点业务互通，业务开通时效建议<分钟级。

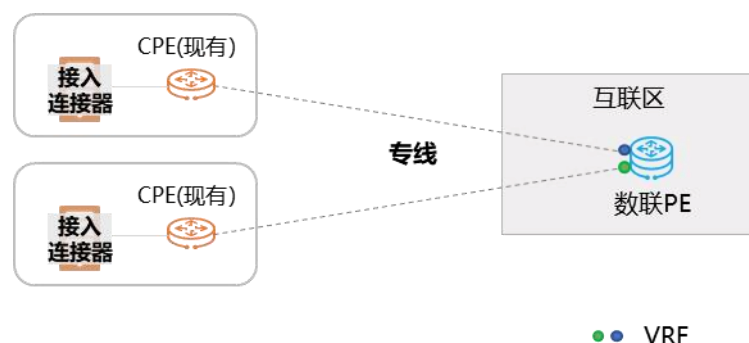


图 8 高速数据流通网络静态接入场景方案图示

8.2.2 关键角色能力要求

静态接入主要通过数联PE提供，要求数联PE具备以下能力：

- a) 应支持基于 IPv6+的灵活组网和 VPN 的路由策略能力；
- b) 应支持 SRv6、随流检测（如 IFIT 等）等技术能力；
- c) 应支持 1G-100G 接入接口，满足多类型带宽接入需求，并支持>400GE 上行带宽，满足海量高质量数据集流通诉求
- d) 应支持识别大象流做负载均衡能力，实现枢纽节点流量均衡调度
- e) 宜支持基于 APN6 的网络标识映射能力，支持数据分级分类与网络标识映射，和出入域管控能力。
- f) 宜支持 IPsec、Xsec、MACsec 等传输加密协议，宜支持量子加密，国密算法、PQC 算法等；

8.3 互联区

8.3.1 网络部署方案

高速数据流通网互联区支撑数据跨网/跨域/跨平台流通的泛在接入，高效流通，交易级建连并满足存证追溯要求。同时互联区需保证用户之间的隔离和数据加密，并且根据数据允许的流通范围控制边界策略。

互联区的数联PE之间（域内/跨域）之间建立SRv6 VPN连接,通过IFIT等随流检测机制实现数据流通可视路径可视，并基于业务安全要求按需完成加密。

互联区与动态专网接入之间有两种对接方式，初期采用跨域VPN的OPTION-A的对接方式：

- a) VPN Option-A模式（背靠背连接）：为避免运营商之间协议交互的开销，业务网关与互联区间采用背靠背组网方式，业务网关用户VPN并建立隧道连通。为实现秒级隧道快速建立能力，运营商业务网关与互联区采用单 VPN 对接架构，完成该运营商下全域数联业务路由学习，同时互联区转发面需基于用户交易，实现用户数据的交易级会话隔离，并具备相应计费统计能力。
- b) 端到端连接：后续互联区可直接贯通企业接入网关、业务网关的SRv6 locator隧道地址，用户VPN连接和传输加密采用端到端方式，实现由数据发送方接入网关至数据接收方接入网关的全程直通。本模式要求接入网关与业务网关之间采用统一协议及标准组网方案，推荐采用SRv6 VPN+APN6+IPSEC6技术组合，以此构建完整的端到端安全连接承载能力。

8.3.2 关键角色能力要求

互联区主要包含接入数联PE，平台PE角色，能力要求包括：

- a) 应支持用户间秒级建连，路由策略控制。
- b) 应支持基于交易的隔离策略，并基于交易进行计费结算。
- c) 宜支持识别大象流做负载均衡能力，实现枢纽节点流量均衡调度
- d) 宜支持基于数网协同标记（如APN6）的出入域管控，控制数据流通范围，如关键数据不能转发到互联网。
- e) 宜支持基于IFIT的路径可视，结合管控层完成路径可视溯源
- f) 宜支持内生的防镜像检测和防分光检测，防止黑客通过分光镜像或远控镜像窃取数据
- g) 宜支持数据传输加密，通过IPSEC6 over SRv6/MACSEC等满足数据加密和按需连的需求。

8.4 网络设施优化能力要求

8.4.1 网络部署方案

运营商网络、行业专网部署独立的三层数联VPN和SRv6隧道承载各企业间的数据流通业务。运营商城域网、行业专网在SRv6隧道上宜部署数网协同功能，基于APN6等关键标识实现基于数据分级分类的差异化选路；同时运营商网络需实现数据的传输路径可视、存证和溯源，并上送运营商控制器提供端到端流通可视。

8.4.2 关键能力要求

网络设施优化的关键能力要求如下：

- a) 宜支持SRv6、基于数网协同标记（如APN6）和网络切片能力，实现差异化路径选路；
- b) 宜支持基于数网协同标记（如APN6）的随流可视并记录路径，结合管控层完成路径可视溯源；
- c) 宜支持内生的防镜像检测和防分光检测，防止黑客通过分光镜像或远控镜像窃取数据；
- d) 宜支持与运营商北向接口对接，下发策略配置并获取路径信息等；

8.5 互联网接入场景

8.5.1 网络部署方案

可以数据基础设施运营方统一建设或各互联网链路服务方独立建设两种模式，见下图：

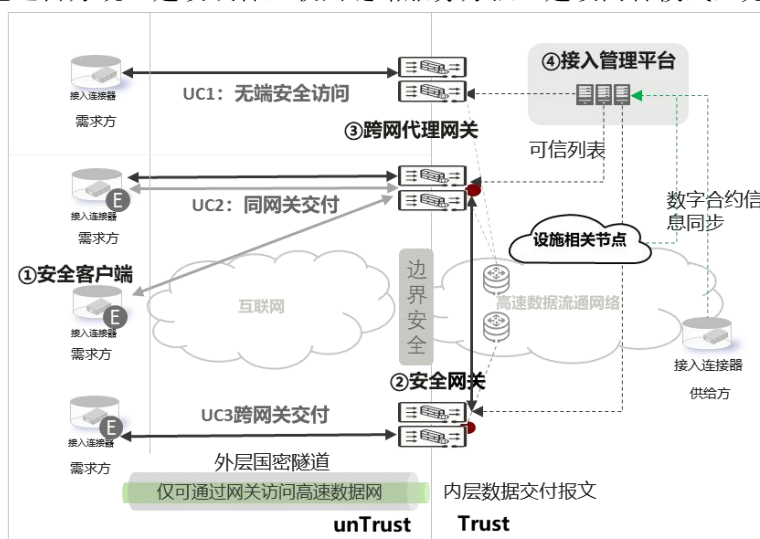


图9 互联网接入核心组件架构

- 安全客户端：部署于接入连接器主机，主要为服务器或云主机。客户端接口应支撑通过接入连接器调用安全客户端的北向接口以发起认证，建立隧道等功能。
- 安全网关：与接入管理平台和安全客户端配合，透明部署或者物理旁路逻辑串联等方式部署于数据流通网互联网边界，实现零信任安全接入放通及威胁攻击行为的阻断。
- 跨网代理网关：与接入管理平台配合，通过凭证校验、代理等技术减少高速数据网的暴露面，实现数据产品级代理（IP、URL等），高速数据流通网内提供方通过跨网代理完成数据交付。
- 接入管理平台：内置于接入管理平台，平台主要负责终端准入、认证鉴权、终端安全隔离、终端安全防护等策略集中制定和下发。平台接口应支持对接统一身份平台实现用户认证、鉴权信息的同步；同时应支持对接基础设施节点实现数据流通授权的获取。

8.5.2 关键能力要求

互联网接入在高速数据流通网络中需部署的关键组件为零信任网关，需满足以下要求：

- 支持通过密码技术或端口敲门技术隐藏安全网关和数据流通专网各类信息化资产；
- 支持通过密码技术保证数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；应当支持国密算法，并满足国家密码应用的标准要求；
- 支持接入连接器接入数据流通专网的源地址代理和源地址转换功能，应支持一一代理和代理后的IP资源静态路由和动态路由功能；
- 支持网关本地和跨网关场景会话表、路由表维护功能，支持静态路由和动态路由功能；
- 支持边界安全能力，包含防火墙，入侵检测，防病毒等能力，应隔离企业之间数据流通的安全威胁。

接入连接器依赖：需具备安全客户端能力，可以通过内置EDR或开发相关模块支持：

- 采用口令认证、密码技术、生物技术等鉴别技术对接入连接器接入数据流通网络进行认证；
- 支持网络隔离，接入连接器获得准入授权后通过安全隧道访问数据流通网络，连接器不可同时访和数据流通网络和互联网；
- 接入连接器通过互联网接入数据流通专网时，实现基于业务需求的访问控制，并实现最小授权；对终端环境进行持续检测和评估，根据评估情况动态调整其应用访问权限。

8.5.3 接入管理平台要求

安全认证授权平台（以下简称“安全平台”）应满足以下要求：

- a) 支持可信资产列表下发安全客户端和安全网关功能；
- b) 支持源地址代理绑定分配功能，宜支持IPv6单栈地址分配；
- c) 按照数据流通任务要求和策略决定，可结合时间窗口和被访问资源粒度，对访问主体授予最小权限。

附 录 A
(资料性)
业务流程示例

A.1 网络能力开通流程

网络能力开通流程用于建立接入连接器与高速数据流通网络之间的接入关系，是数据流通业务使用高速数据流通网络的前置条件。流程涉及用户、接入连接器、数据基础设施相关节点、网络调度平台和运营商网络控制器五类角色。网络服务开通与注销流程见图10。

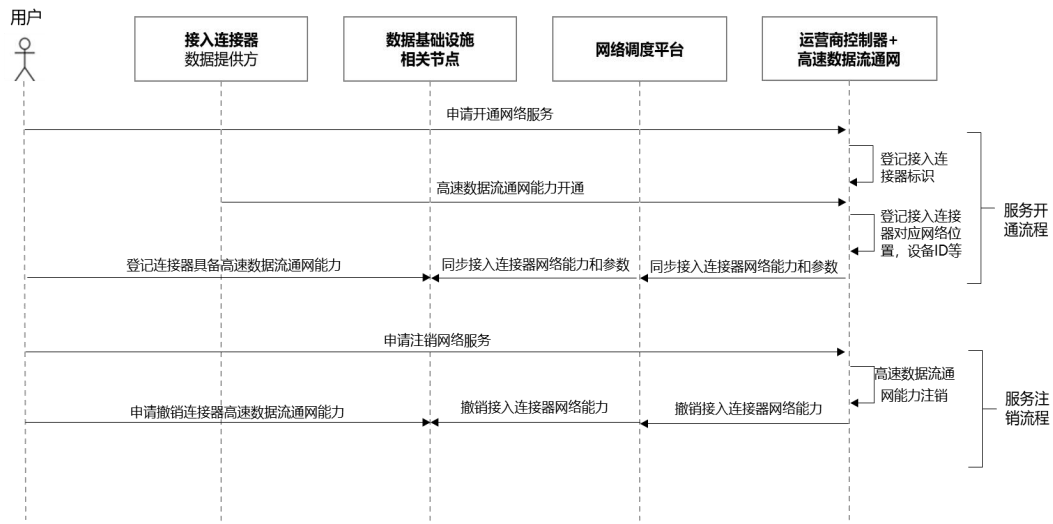


图 10 用户高速数据流通网络服务开通/注销流程图

- 申请开通：用户通过运营商申请高速数据流通网络服务开通，申请内容包括接入主体信息、接入连接器标识、接入方式、开通地点和带宽等接入需求；
- 配置开通：运营商网络完成该接入连接器的可信接入网关、业务网关及城域网的相关配置，并为接入连接器分配 IP 地址；
- 能力开通同步：运营商控制器和网络调度平台通过北向网络能力开通接口操作的结果同步，向数据基础设施相关节点回传该接入连接器的运营商网络能力信息和接入参数，建立接入连接器标识与 IP 地址的绑定关系；
- 登记完成：数据基础设施相关节点登记该接入连接器具备高速数据流通网络能力，是否双网络接入（高速数据流通网+互联网），开通流程结束。

A.2 网络能力注销流程

网络服务注销流程用于解除接入连接器与高速数据流通网络之间的接入关系，流程见图6。服务注销流程说明如下：

- 申请注销：用户向对应运营商提交网络服务注销申请；
- 能力注销：运营商网络控制器解除相关网络配置、释放网络资源，并通过该接口操作的结果同步向网络调度平台回传注销结果；
- 能力撤销：网络调度平台撤销该接入连接器的网络能力登记和绑定关系，并通过北向网络能力拆除接口操作的结果同步，向数据基础设施相关节点回传撤销结果；
- 撤销完成：数据基础设施相关节点撤销该接入连接器具备高速数据流通网络能力的登记，清理其网络能力信息，注销流程结束。

A.3 网络服务按需调用流程

网络服务按需调用流程用于在数据供需双方达成数据流通交易后，按交易需求建立数据供给方接入连接器与数据订购方接入连接器之间的连接。流程的前置条件是数据供需双方接入连接器均已完成网络服务开通。网络服务按需调用与服务结束撤销流程见图11。

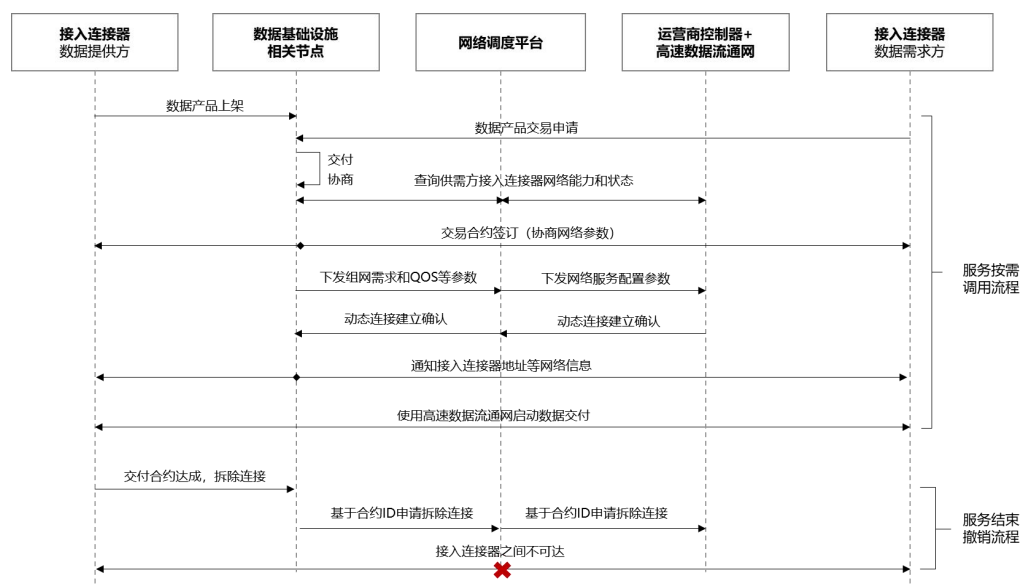


图 11 高速数据流通网络按需调用流程图

服务按需调用流程说明如下：

- 产品上架：数据供给方通过接入连接器向数据基础设施相关节点上架数据产品，并在数据产品中明确可通过高速数据网或高速数据网+互联网（纯互联网场景遵循现有流程），以及网络带宽、时延等网络要求；对于高速数据网+互联网数据产品，设施节点将该数据产品同步到接入管理平台登记，完成代理网关策略下发。
- 交易申请：数据需求方通过接入连接器向数据基础设施相关节点提交数据产品使用申请。
- 交付协商：数据供需方协商使用高速数据流通网络进行数据交付；
- 能力核对：数据基础设施相关节点通过状态查询接口核对数据供需双方接入连接器的网络能力和网络接入状态，确认双方均具备组网条件。（对于需方连接器不具备高速数据网能力的，若数据产品可通过互联网访问则重新协商互联网+反向代理模式交付，交付策略下发代理网关）
- 合约签订：数据供需双方通过数据基础设施相关节点签订数据流通交易合约，并约定本次数据交付所需的网络参数；
- 需求下发：数据基础设施相关节点调用动态组网需求分发接口向网络调度平台下发组网需求，携带合约标识、供需双方接入连接器标识、服务质量参数和连接有效期等要求；
- 参数下发：网络调度平台将组网需求转换为网络控制策略，调用动态组网配置分发操作分别向供需双方所属的运营商网络控制器下发网络参数；
- 配置执行：运营商网络控制器完成路由策略发布、隧道建立、隔离策略和带宽保障配置后，调用南向动态连接建立确认接口操作向网络调度平台确认本侧连接建立结果；
- 连接确认：网络调度平台汇总数据供需双方各侧的确认结果并完成连通性确认后，调用北向动态连接建立确认接口操作向数据基础设施相关节点回传连接标识、连接状态和双方 IP 地址等信息；

- j) 地址获取：数据基础设施相关节点将对端网络地址等网络信息通知数据供给方和数据订购方的接入连接器，或接入连接器通过对端接入连接器 ID 获取对端接入连接器地址；
- k) 数据交付：接入连接器完成地址配置后，使用高速数据流通网络启动数据交付。

A. 4 服务结束撤销流程

服务结束撤销流程用于在数据交付完成后拆除数据供需双方接入连接器之间的连接，流程见图11。
服务结束撤销流程说明如下：

- a) 拆除申请：数据交付完成、交付合约达成后，数据基础设施相关节点调用基于合约标识申请拆除连接接口操作向网络调度平台提交拆除申请，携带合约标识；
- b) 拆除下发：网络调度平台受理拆除申请，调用南向基于合约标识申请拆除接口操作向相关运营商网络控制器下发拆除配置；
- c) 配置撤销：运营商网络控制器撤销相关路由策略、隧道和隔离策略，释放带宽资源，并通过南向基于合约标识申请拆除连接接口操作的结果同步向网络调度平台回传本侧拆除结果；
- d) 拆除完成：网络调度平台汇总各侧拆除结果后，通过北向基于合约标识申请拆除接口操作的结果同步向数据基础设施相关节点回传，数据基础设施相关节点通知数据供给方和数据订购方的接入连接器；
- e) 恢复隔离：拆除完成后，数据供给方与数据订购方的接入连接器之间恢复为不可达状态，双方各自与高速数据流通网络之间的网络能力保持不变。

附 录 B
(资料性)
南北向交互接口参数

B.1 网络能力开通

用于运营商控制器向网络调度平台，以及网络调度平台向数据基础设施相关节点同步接入连接器对应的高速数据流通网络能力开通情况。

调用方：网络调度平台/运营商控制器
同步参数见表1。

表 1 网络能力开通同步参数

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	接入连接器标识	connectorId	String	32	必选	接入连接器的全局唯一标识,应与用户身份管理体系中登记的接入连接器标识一致
2	接入主体名称	subjectName	String	100	可选	接入连接器所属接入主体的名称
3	接入方式	accessType	String	2	M	0-动态专网接入；1-静态专线接入；
4	接入网络提供方标识	operatorId	String	32	必选	为接入连接器提供接入网络的运营商或行业专网责任主体的标识
5	开通地点	accessLocation	String	200	可选	接入连接器的网络接入地点，包括省、市及详细地址
6	最小带宽	Minbandwidth	Integer	10	必选	可调度的最小带宽值
7	最大带宽	maxbandwidth	Integer	10	必选	可调度的最大带宽值
8	带宽单位	bandwidthUnit	String	2	必选	枚举：M、G

数据基础设施相关节点收到结果同步后，应登记该接入连接器具备高速数据流通网络能力，并留存其运营商网络IP地址和网络能力信息，作为后续下发组网需求的依据。

B.2 网络能力注销

该接口操作用于运营商控制器向网络调度平台以及网络调度平台向数据基础设施同步网络能力注销信息。

调用方：网络调度平台/运营商控制器
请求参数见表2。

表 2 网络能力拆除同步参数

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	接入连接器标识	connectorId	String	32	必选	待注销网络能力的接入连接器标识
2	接入网络提供方标识	operatorId	String	32	必选	待注销的运营商网络端点IP节点
3	注销原因	terminationReason	String	200	可选	网络能力注销的原因说明

数据基础设施相关节点收到结果同步后，应撤销该接入连接器具备高速数据流通网络能力的登记，并清理其运营商网络IP和网络能力信息。

B.3 动态组网需求分发

该接口操作用于数据基础设施相关节点在数据供需双方签订交易合约后，向网络调度平台下发组网需求，结合配置分发接口操作，建立数据供给方接入连接器与数据订购方接入连接器之间的连接。

调用方：数据基础设施相关节点

响应方：网络调度平台

参数见表3。

表 3 动态组网需求分发参数

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	合约标识	contractId	String	32	必选	数据流通交易合约的全局唯一标识，作为本次组网及后续连接拆除、状态查询和信息上报的业务关联标识
2	数据供给方接入连接器标识	providerConnectorId	String	32	必选	数据供给方接入连接器的接入连接器标识
3	数据供给方接入连接器IP	providerConnectorIp	String	128	可选	数据供给方接入连接器本次组网所使用的IP地址
4	数据供给方接入网络提供方标识	providerOperatorId	String	32	必选	数据供给方运营商网络端点所属的接入网络提供方标识
5	数据订购方接入连接器标识	consumerConnectorId	String	32	必选	数据订购方接入连接器的接入连接器标识
6	数据订购方运营商网络端点IP节点	consumerConnectorIp	String	128	可选	数据订购方接入连接器本次组网所使用的IP地址
7	数据订购方接入网络提供方标识	consumerOperatorId	String	32	必选	数据订购方运营商网络端点所属的接入网络提供方标识
8	带宽	bandwidth	Integer	10	必选	本次连接所需的带宽数值
9	带宽单位	bandwidthUnit	String	2	必选	枚举：M、G
10	时延	latency	Integer	10	可选	本次连接的端到端时延要求，单位为毫秒；数据流通业务提出实时性要求时必须填
11	安全等级	securityLevel	String	2	可选	0—一般；1—重要；2—加密；

B.4 动态组网配置下发

该接口操作用于网络调度平台将组网需求转换后的网络控制策略下发至运营商网络控制器。

调用方：网络调度平台

响应方：运营商网络控制器

参数见表4。

表 4 下发网络服务配置参数请求参数

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	连接标识	connectionId	String	32	必选	网络调度平台生成的连接唯一标识，用于本连接全生命周期的关联，可以与合约标识相同
3	数据供给方接入连接器标识	providerConnectorId	String	32	必选	数据供给方接入连接器的接入连接器标识
4	数据供给方接入连接器IP	providerEndpointIp	String	128	必选	数据供给方接入连接器IP地址

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
5	数据供给方网关IP地址	providerEndpointIp	String	128	可选	数据供给方运营商控制连接的网关地址（可信接入网关/业务网关）
6	数据订购方接入连接器标识	consumerConnectorId	String	32	必选	数据订购方接入连接器的接入连接器标识
7	数据订购方接入连接器IP	consumerEndpointIp	String	128	必选	数据订购方接入连接器IP地址
8	数据订购方网关IP地址	consumerEndpointIp	String	128	可选	数据订购方运营商控制连接的网关地址（可信接入网关/业务网关）
9	本侧角色	localRole	String	2	必选	本运营商网络控制器在本次连接中承担的侧别，0-数据供给方侧；1-数据订购方侧；2-数据供需双方同侧
10	带宽	bandwidth	Integer	10	必选	本次连接所需的带宽数值
11	带宽单位	bandwidthUnit	String	2	必选	枚举：M、G
12	时延	latency	Integer	10	可选	本次连接的端到端时延要求，单位为毫秒；数据流通业务提出实时性要求时必须填
13	安全	securityLevel	String	2	可选	0-无特殊配置；1-切片隔离；2-传输加密；

B.5 动态组网建立确认

该接口操作用于运营商网络控制器在完成本侧网络服务配置后，向网络调度平台确认本侧动态连接的建立结果，以及网络调度平台在汇总数据供需双方所属运营商网络控制器的配置执行结果并完成连通性确认后，向数据基础设施相关节点确认动态连接的建立结果。

调用方：运营商控制器，网络调度平台。

参数见表5。

表 5 动态连接建立确认请求参数

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	合约标识	contractId	String	64	必选	本次连接所对应的数据流通交易合约标识
2	连接标识	connectionId	String	64	可选	待确认的连接标识，与动态组网组网需求参数中的连接标识一致
3	连接状态	connectionStatus	String	2	必选	1-已建立或4-异常
4	数据供给方接入连接器标识	providerConnectorId	String	32	必选	数据供给方接入连接器的接入连接器标识
5	数据订购方接入连接器标识	consumerConnectorId	String	32	必选	数据订购方接入连接器的接入连接器标识
6	生效带宽	bandwidth	Integer	10	可选	连接实际生效的带宽数值，连接状态为已建立时必须填
7	带宽单位	bandwidthUnit	String	2	可选	枚举：M、G；连接状态为已建立时必须填
8	连接生效时间	effectiveTime	String	19	必选	连接实际生效时间，格式为yyyy-MM-dd HH:mm:ss；连接状态为已建立时必须填
9	失败原因	failureReason	String	200	可选	连接状态为异常时必须填，说明连接建立失败的原因

B.6 动态组网拆除连接

该接口操作用于数据交付完成后，数据基础设施相关节点基于合约标识向网络调度平台申请拆除数据供需双方接入连接器之间的连接。

调用方：数据基础设施相关节点，网络调度平台

响应方：运营商网络控制器，网络调度平台

参数见表6, 7

表 6 动态组网拆除请求参数

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	合约标识	contractId	String	64	必选	本次连接所对应的数据流通交易合约标识
2	连接标识	connectionId	String	64	可选	待确认的连接标识，与动态组网组网需求参数中的连接标识一致
3	数据供给方接入连接器标识	providerConnectorId	String	32	必选	数据供给方接入连接器的接入连接器标识
4	数据订购方接入连接器标识	consumerConnectorId	String	32	必选	数据订购方接入连接器的接入连接器标识

表 7 响应参数

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	合约标识	contractId	String	64	必选	与请求参数一致
2	连接标识	connectionId	String	64	必选	与请求参数一致
3	配置执行状态	configStatus	String	2	必选	1-配置成功 2-配置失败
4	拆除完成时间	releaseTime	String	19	可选	本侧连接实际拆除完成时间，格式为 yyyy-MM-dd HH:mm:ss；配置执行状态为配置成功时必填
5	失败原因	failureReason	String	200	可选	配置执行状态为配置失败时必填，说明本侧拆除失败的原因

B.7 网络能力和状态查询

该接口操作用于数据基础设施相关节点向网络调度平台查询接入连接器的网络能力、网络接入状态、连接状态以及网络质量和流量信息等。

调用方：数据基础设施相关节点，网络调度平台

提供方：网络调度平台。

请求参数见表8。

表 8 网络能力和状态查询请求参数

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	状态类型	statusType	String	2	必选	0-网络能力和接入状态；1-连接状态；2-流量信息
2	接入连接器标识	connectorId	String	32	必选	状态类型为0时必填；支持填写多个，以逗号分隔，用于一次核对数据供需双方的网络能力
3	接入连接器IP地址	connectorIP	String	128	可选	按运营商网络端点查询时必填

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
4	接入网络提供方标识	operatorId	String	32	必选	为接入连接器提供接入网络的运营商或行业专网责任主体的标识
5	查询开始时间	startTime	String	19	可选	状态类型为2、3时必填，格式为yyyy-MM-dd HH:mm:ss
6	查询结束时间	endTime	String	19	可选	状态类型为2、3时必填，格式为yyyy-MM-dd HH:mm:ss
7	统计时间粒度	timeGranularity	String	8	可选	状态类型为2、3的统计粒度，枚举：5min、1h、1d

响应参数见表9。

表 9 网络能力和状态查询响应参数

序号	中文名称	字段名称	数据类型	长度	约束类型	取值说明
1	状态信息	status	String	2	M	0-不具备能力，1-连接状态正常
2	记录总数	totalCount	Integer	10	M	符合查询条件的记录总数
3	采集时间	collectTime	String	19	M	查询结果的信息采集时间，格式为yyyy-MM-dd HH:mm:ss
4	采集来源	collectSource	String	64	M	查询结果的信息采集来源，取值为网络调度平台或相应的接入网络提供方标识

参 考 文 献

- [1] 国家数据基础设施建设指引（发改数据〔2024〕1853号）
 - [2] 数据领域常用名词解释（第一批）（国家数据局）
 - [3] 数据领域常用名词解释（第二批）（国家数据局）
 - [4] GB/T 41479-2022 信息安全技术 网络数据处理安全要求
 - [5] GB/T 43697-2024 数据安全技术 数据分类分级规则
 - [6] GB/T XXXXX-XXXX 《数据 基础术语》
 - [7] GB/T XXXXX-XXXX 《数据基础设施 参考架构》
 - [8] GB/T XXXXX-XXXX 《数据基础设施 互联互通基本要求》
 - [9] GB/T XXXXX-XXXX 《数据基础设施 用户身份管理和接入要求》
 - [10] GB/T XXXXX-XXXX 《数据基础设施 连接器技术要求》
 - [11] GB/T XXXXX-XXXX 《数据基础设施 标识要求》
-