智能体互联网愿景及关键技术白皮书

1. 引言

在数字时代的浪潮中，互联网作为全球信息交互与资源配置的核心基础设施，已深刻影响了人类社会的生产生活方式。从早期的文本交互到如今的多媒体应用，从固定终端接入到移动互联普及，互联网经历了数次迭代演进，不断拓展着连接的边界与服务的深度。随着人工智能、大数据等新兴技术的迅猛发展，算力资源需求激增，算力成为互联网体系结构中的新要素，传统互联网基础设施之上催生出算力网络的新体系和新服务，持续释放算力效能。

随着智能体技术的深入发展，更进一步激发了数字经济对高效协作、个性化服务、自主化管理的新需求。而当前以平台为中心、以人类主导操作为核心的互联网体系正面临重重挑战，亟待变革。“数据孤岛”让不同平台、不同系统之间的信息流通共享受阻，资源配置效率低下。用户在获取服务时需主动在多个平台间切换操作，交互流程繁琐，难以获得精准、无缝的个性化体验。此外，面对日益复杂的网络环境和海量的网络设备，传统人工主导的网络管理模式已难以应对，网络的可靠性、安全性和智能化水平亟待提升。在此背景下，**智能体互联网**（Internet of Agents，IoA）应运而生。**作为新质互联网的具象化体现，智能体互联网是基于当前互联网基础设施构建的新型网络，绝非简单的技术叠加，而是对互联网体系结构的有效补充，丰富了互联网的运行逻辑与价值范式，将深刻影响互联网基础设施、技术应用、产业生态等多个层次和维度，成为数智时代的核心技术标志。**

智能体互联网顺应数字经济发展的时代需求而提出，在基础设施

层面，它将推动网络从“管道化”向“智能化”升级，重塑网络的连接、计算与存储体系；在产业范式层面，它将打破传统产业的边界限制，催生“智能体协同”的新型产业生态，重塑产业链、供应链与价值链；在应用业态层面，它将从根本上改变服务的生产与交付方式，催生一批全新的智能应用场景，将推动全方位提升开放协作、高效的网络生态。在个人层面，智能体互联网将为用户提供全方位、个性化的智能服务，极大提升生活便捷性与幸福感；在社会层面，它将助力智慧城市、智能交通等公共服务领域的智能化升级，提高社会运行效率与治理水平。

本白皮书旨在系统阐述智能体互联网的发展愿景、架构体系、关键技术及典型应用场景，明确智能体互联网的发展方向与路径，为政府部门、科研机构、产业界等相关主体提供参考，凝聚发展共识，共同推动智能体互联网的研发与应用落地，助力数字经济高质量发展。

2. 智能体互联网发展愿景

2.1. 定义与内涵

智能体互联网是一种以智能体（Agent）为核心互联主体，通过统一的协议、接口，实现智能体之间、智能体与用户、智能体与工具之间自主发现、高效交互、协同协作的新型互联网基础设施，是新质互联网的具象化演进目标之一。其中，智能体是指具备感知、决策、执行、学习等自主能力，能够根据环境变化和目标需求自主完成任务的实体，既可以是虚拟的软件程序，也可以是智能硬件物理设备。

从内涵上看，智能体互联网并非对现有互联网的颠覆，而是在现有互联网基础上的延伸与升级。它打破了传统互联网中以人类用户为核心交互对象的局限，将智能体纳入互联体系，形成了人类与智能体协同共生的新型网络生态。在这一生态中，智能体不仅是信息的传递者和服务的提供者，更是自主的决策者和协作者，能够代表人类或其他实体完成复杂的任务，实现资源的优化配置和服务的精准交付。

智能体互联网的目标愿景是构建一个开放协作、安全高效、高度智能的网络环境，形成全新的人智协同范式，极大地解放人类生产力，深化生产关系变革，促进人类社会高质量发展。它强调以用户需求为导向，通过智能体之间的自主协作，降低用户的操作成本，提升服务的个性化和智能化水平。同时，智能体互联网注重打破数据和服务的壁垒，实现跨平台、跨领域的资源共享，推动创新要素的自由流动。

2.2. 核心特征

2.2.1. 新互联主体

在传统互联网架构中，人类是绝对的核心互联主体，网络设计、服务提供和交互方式均以人类用户为中心展开。用户需要主动搜索信息、选择服务、完成操作流程，网络的智能化程度较低，主要起到信息传递和资源聚合的作用。

而在智能体互联网中，互联主体发生了根本性转变，将向人类与智能体协作共生的“人智协同”模式演进。智能体能够感知用户需求，代表用户完成信息筛选、服务匹配、任务执行等一系列操作，成为与人类同等重要的互联主体。人类用户则从繁琐的具体操作中解放出来，更多地承担目标设定、决策监督和结果评价的角色。

智能体作为一种新的互联主体，不仅为互联网带来了新服务，也引发了互联网为其演进升级的新变革。网络要理解智能体与传统人类的差别，就需要新的身份标识和发现机制；智能体代表人类执行操作，以及智能体之间进行任务协作也需要互联网为两种不同的实体定义差异化的权限范围和执行逻辑。

2.2.2. 新交互范式

交互范式的演进是互联网发展的重要标志之一。在互联网起步阶段，“WebUI”是典型的交互范式。用户在互联网主要采用文本/超文本进行交互，互联网 Web 网页是用户获取信息的唯一入口。用户通过点击文本链接获取信息的方式单一、直观性差，用户体验较为有限。随着移动互联网时代的到来，图形用户界面“GUI”成为主流交互范

式，用户借助手机、PC 等终端设备通过窗口、图标、菜单、指针等可视化元素访问互联网，极大提升了交互的直观性和便捷性，推动了互联网的普及应用。

智能体互联网将催生全新的交互范式，即**多模态用户界面“MUI”。**它融合了语音、图像、视觉等多种感知模态，实现了更加自然、高效、个性化的人机交互。MUI 不再局限于传统的鼠标、键盘、触屏操作，用户可以通过语音指令与智能体交流，通过图像识别让智能体理解视觉信息，通过手势动作向智能体传达意图，甚至可以通过表情识别实现情感层面的交互。

MUI 交互范式的核心优势在于其高度的自然性和适应性，极大的贴合了人类原生的交互方式。它能够根据用户的使用习惯、场景需求和生理特征，自动调整交互方式，为不同用户提供个性化的交互体验。例如，在驾驶场景中，用户可以通过语音指令控制车载智能体完成导航设置、音乐播放等操作，无需分心操作触摸屏；在智能家居场景中，用户可以通过手势动作控制家居智能体开关灯、调节温度等，实现更加便捷的家居控制。

2.2.3. 新协作模式

传统协作模式中，人类作为绝对操作和决策主体，需全程主导任务规划、执行与流程管控，从基础数据处理到复杂业务逻辑梳理均依赖人力。这不仅耗费大量精力，更受限于人类认知边界，在大规模、高复杂度任务中效率与精准度瓶颈凸显。

智能体互联网彻底重构了协作逻辑，**推动人类定位从“操作主体”向“决策主体”转变，**智能体则承担起任务执行逻辑的核心制定职责。**这种“人智协同”的模式实现了人类智能与人工智能的优势互补。**

人与智能体协作层面，智能体主要进行操作，人类主要进行决策。智能体依托算法模型与知识储备，快速拆解任务目标、规划执行路径、分配资源，形成完整执行方案。人类仅需在战略方向、核心决策等关键环节提供经验指导，无需介入具体操作。

智能体与智能体相互协作层面，智能体之间进行合理的任务分工，通过形成工作流驱动多智能体实现高效链式协作。前一智能体完成子任务后，自动触发下一智能体的工作流程，实现信息与结果的无缝传递。以电商供应链为例，订单智能体接收订单后同步至库存智能体，库存智能体判断缺货后触发采购智能体启动供应商筛选与下单流程，全链路无需人工干预，大幅提升供应链响应效率。

这种“智能执行 + 人类决策”的协作模式，实现了人机优势互补：智能体承接重复性、规律性工作，释放人力；人类聚焦创造性、战略性高价值任务。最终推动工作效率与创新能力双重提升，成为各行业数字化转型的核心驱动力。

2.2.4. 新资源抽象

传统互联网的资源体系中，数据与算力占据核心地位，传统概念中的“工具”仅作为辅助手段存在（如软件开发套件），高度依赖人工操作才能发挥作用，其价值与使用者技能深度绑定。这种定位限制

了工具的使用门槛和价值空间。

智能体互联网彻底重塑了这一资源格局，“工具”被提升到核心地位，实现对数据、算力等资源要素的高度抽象和动态使用。通过标准化封装，工具摆脱了对人工的依赖，成为智能体可自主调用、灵活组合、高效复用的关键资源，**呈现出数据工具化、功能工具化、服务工具化的特点，**让静态数据变为动态工具，传统数据多以原始形态存储，需人工分析才能释放价值，而数据工具化依托智能体自动完成数据清洗、特征提取，并与算法模型封装为标准化“数据工具模块”。例如工业场景中，设备传感器采集的原始数据经处理后成为“故障预警工具”，生产调度智能体调用即可快速获取设备健康评估，无需自行处理海量数据。

作为核心资源抽象，工具是智能体能力的关键赋能载体。单一智能体通过调用工具可快速拓展能力边界，如家居智能体借助环境监测、能耗分析工具实现综合管控；跨领域智能体依托共享工具池实现协同创新，如农业与气象智能体共享分析工具优化种植方案。统一的封装标准将促进形成“开发 - 调用 - 迭代”的良性生态，为智能体互联网的规模化落地提供持续动力。

3. 典型场景

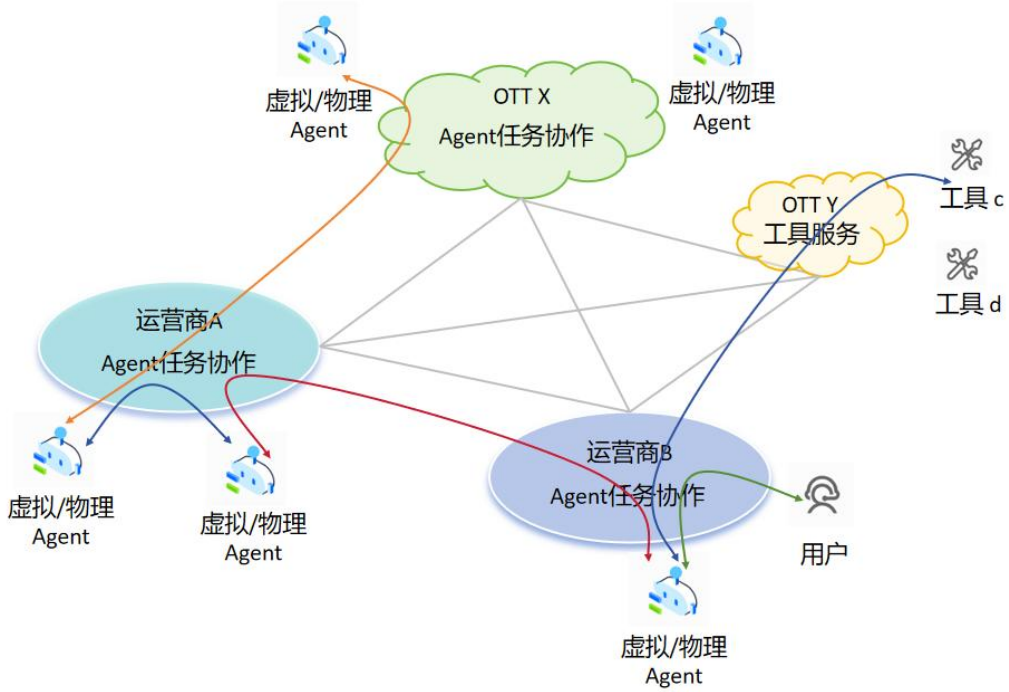

图 3-1 智能体互联网典型场景互联关系示意

图 3-1 展示了智能体互联网典型场景中三种主要的互联关系以及场景细化后的互联示意。其中三种主要的互联关系，包括**用户与智能体、智能体与智能体、以及智能体与外部工具**。这三种互联关系还能够根据场景要求进一步细分。例如智能体与智能体互联方面，首先智能体类型可以细分为物理智能体（如具身智能）和虚拟智能体（如 AI 软件助手）；在网络域方面，可以分为域内网络（如单运营商网络）和跨域/域间网络（如跨运营商网络，或者跨运营商和 OTT 云商网络）。因此，图 4-1 显示的智能体互联关系呈现多样化。4.1 和 4.2 章节将分别以虚拟智能体助手和物理智能体协作两个代表性的场景示意智能体的互联关系和应用。其中 4.1 章节中展示的虚拟智能体助手场景中，以车载语音助手为例，介绍了智能体自动预订酒店服务的场景，这其

中包含了人与虚拟智能体、虚拟智能体与虚拟智能体、虚拟智能体与工具之间互联或调用关系。而在 4.2 章节，具身智能体协作案例中，显示了具身智能体（机器狗或无人机）之间、具身智能体与人类、具身智能体与工具的各类连接关系。

3.1. 人类虚拟智能体助手

场景概述

在智能网联汽车上，用户无需点击屏幕或切换 App，只需自然对话与车辆系统 Agent 交互，多个服务 Agent 即可协同完成任务。比如，用户正在驾驶车辆，无法直接操作手机，用户询问车载智能语音助手，帮忙预订目的地的酒店。随后车载智能体与后端地图服务智能体、酒店管理服务智能体、支付服务智能体等进行通信协作，共同完成酒店自动化筛选和预订任务。

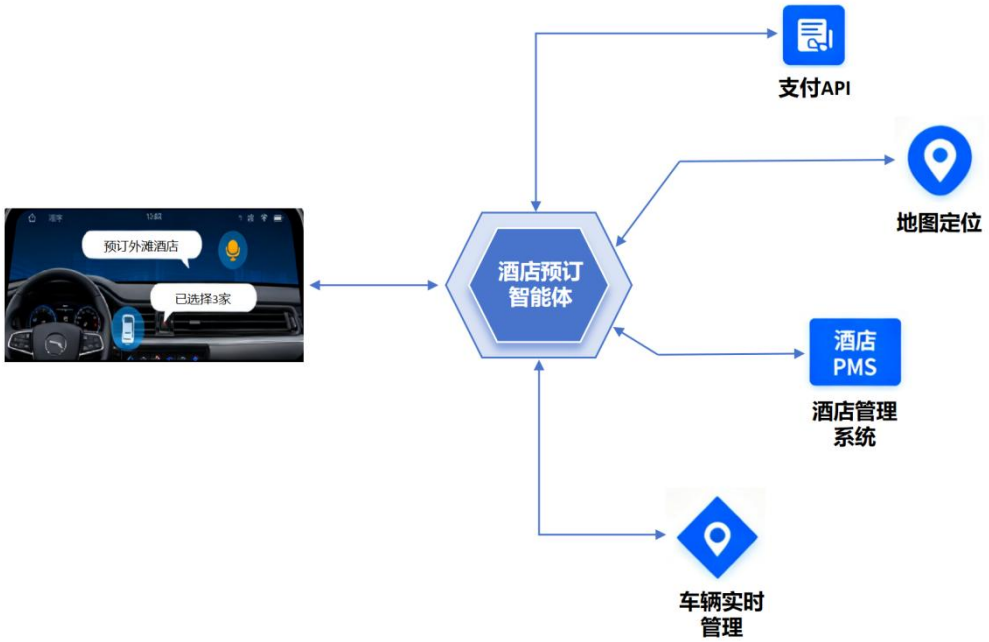

图 3-2 人类虚拟智能体协作场景示意

核心角色

车辆智能语音助手：负责接受用户意图，与服务 Agent 交互完成业务闭环

酒店预订服务智能体：负责接受系统 Agent 的指令，完成该服务垂域的业务，并和其他服务 Agent 交互

协同流程

酒店预订管理：

步骤 1：用户唤醒车机，通过语音向车辆系统 Agent 发出意图：“出差行程安排”

步骤 2：系统 Agent，通过多智能体协同架构，实现多模态交互与 AI Agent 集群协作；

步骤 3：系统 Agent 调用导航、酒店预订管理、支付服务、充电桩预约等多个服务 Agent 协同响应，形成场景化服务闭环。

3.2. 物理智能体任务协作

场景概述

在户外安防地场景中，用户通过语音启动智能巡逻，机器狗自主覆盖场地边界并实时回传 4K 画面至家庭 AI 服务器。家庭 AI 服务器自动识别入侵者或环境异常，推送告警至用户终端，支持语音指令远程驱赶，或联动无人机接力追踪，实现“发现风险—即时响应—动态防御”闭环，提升私密露营与园区等场景的安全性。

图 3-3 物理智能体协作场景示意

核心角色

机器狗：搭载 4K 摄像头、红外传感器、扬声器与闪光灯，具备自主导航与环境感知能力，接入移动核心网。负责区域巡逻，执行驱赶、警示、视频上传任务。

家庭 AI 服务器：部署于家中，作为算力中枢处理视频流，执行 AI 分析与任务调度，实现与用户终端的低时延直连。

个人终端：接收原始 4K 视频与告警，支持语音指令指挥设备（如“驱赶闯入者”）。

无人机：覆盖机器狗盲区（高空/密林），执行接力追踪任务。

协同流程

任务启动与智能巡逻

步骤 1：用户通过语音或 APP 发起“启动露营地巡逻”指令，经核心网下发至机器狗；

步骤 2：机器狗启动自主巡逻，动态规划路径，避开障碍物并优先覆盖高风险区域；

步骤 3：机器狗接入核心网，持续回传 4K 视频流至家庭 AI 服务器。

智能分析与风险识别

步骤 1：家庭 AI 服务器接收视频流，本地实时分析：目标识别、行为判断、环境预警；

步骤 2：系统判定风险等级，生成相应策略；

步骤 3：高风险事件立即触发告警推送流程。

低时延告警与用户直连交互

步骤 1：家庭 AI 服务器通过 UPF 直连，将 4K 视频与告警信息实时推送至用户终端；

步骤 2：用户实时查看现场，通过语音指挥机器狗执行播放警示语音、启动闪光灯、调整巡逻路径、110 报警等；

步骤 3：联动无人机覆盖盲区或用户指定区域，执行接力追踪或执行特定任务，形成空地协同防御。

4. 智能体互联网架构与关键技术

当前互联网基础设施基于 TCP/IP 协议栈实现了海量终端设备与大型数据中心的高效互联，并在物理资源之上构建起虚拟化的云互联网络。而智能体互联网在传统互联网基础设施之上需要实现**智能体互**

联互通和智能体任务协作两大目标。这就带来了组网架构的新需求和新变化。

在组网范围层面，一方面是单域内智能体互联互通，典型应用场景包括在 6G 通信网络内的任务式自组网。单域内智能体的身份标识和授权可以由该域的服务提供者统一管理，提供权威认证。**另一方面是跨域的智能体互联互通，**典型场景包括跨 OTT 服务提供商网络进行智能体协作。跨域的场景下需要由第三方权威机构提供标识的解析，同时智能体在请求其他智能体的操作权限时，往往还需要智能体所属用户的参与和授权。

在架构特性层面，当前互联网体系架构呈现出明显的“平台为中心”特征，大型互联网服务提供商凭借其强大的资源整合能力和用户聚合能力，掌握了信息分发、服务提供和数据管理的核心权力，虽然在可管理性方面具有优势，但也在一定程度上带来数据孤岛、竞争壁垒等问题。**智能体互联网将驱动互联网回归“去中心化”的本质。**随着智能体应用场景的不断扩展，智能体跨主体协作、跨多云协作将成为未来发展新模式，智能体应用将逐步弥合大型平台之间的互联协作鸿沟，极大的提升用户服务体验和协作效率。

在协议体系方面，智能体互联网是构建于传统互联网 TCP/IP 五层协议（物理层、数据链路层、网络层、传输层、应用层）之上，实现智能体高效互通的新体系。传统 5 层协议主要解决了面向主机之间通信的数据传输问题。而智能体互联网在应用层之上，**构建了“新 5 层”协议体系**。面向智能体新增了身份标识、语义互通等功能，以满足智

能体之间自主发现、安全交互和协同协作的需求。

4.1. 智能体互联网总体架构和技术体系

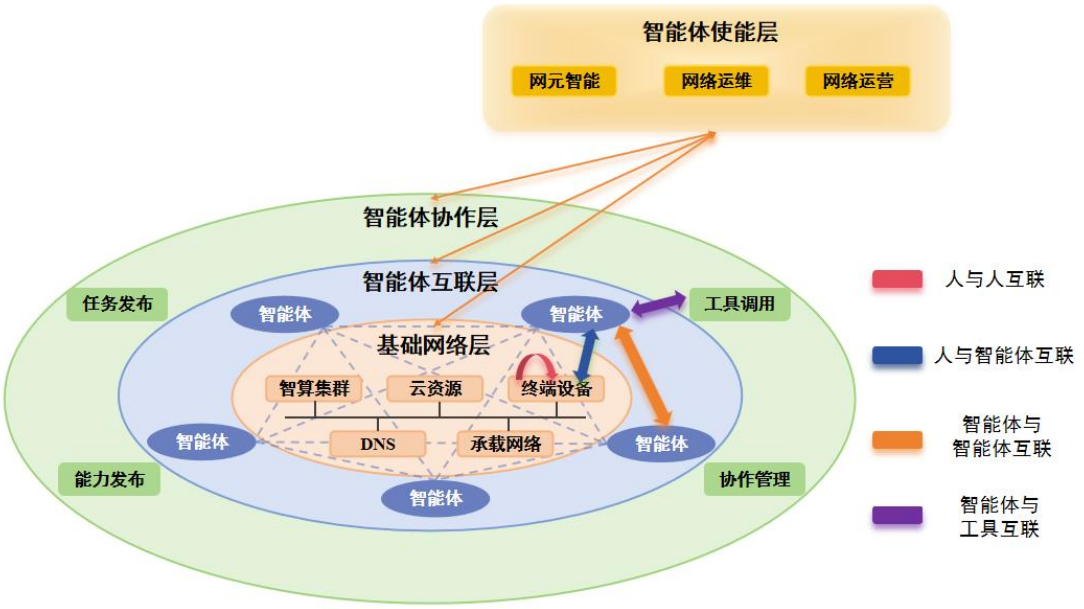

图 4-1 智能体互联网总体架构设想

智能体互联网总体架构包含**三个互联层面、四种互联关系，以及一个管理平面**。三种互联关系包括传统互联网实现的人与人互联，而智能体互联网带来了智能体与人的互联以及智能体之间的互联关系。互联层次方面，实现人与人互联的是底层的基础互联网络层，这一层主要使能技术或协议包括 IPv4/IPv6、DNS、BGP/IGP 等。在其之上构建的是智能体互联层，主要实现的是智能体的身份标识、身份发现、智能体路由等功能。最上层是智能体任务协作层，主要实现面向特定任务的智能体认证授权、能力发布和协作等。一个管理平面指的是智能体赋能网络管控，智能体作为网络内部的核心组件，实现网络监控和闭环保障的功能，将充分实现意图驱动，引领网络走向高阶自智。

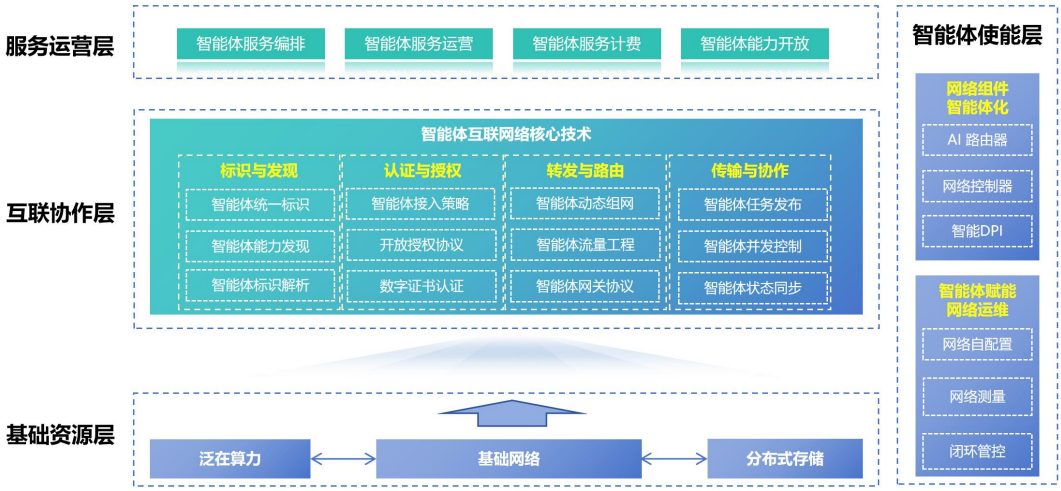

图 4-2 智能体互联网关键技术体系示意图

面向智能体互联网架构设想，图 4-2 进一步呈现了未来智能体互联网的关键技术体系。其中智能体带来最大的变化在于互联协作层和智能体使能层。在智能体互联协作层中，需要围绕标识发现、认证授权、转发路由、传输协作等关键技术进行设计。而智能体使能层则主要覆盖两个方面，包括网络组件智能体化，以及智能体赋能网络运维，升级现有网络运维体系。4.2 和 4.3 章节将分别从智能体互联协作、智能体赋能网络两个维度深入介绍关键使能技术。

4. 2. 智能体互联关键技术方向

4.2.1. 标识发现

功能需求

智能体标识：智能体网络互联初期仍依托广域 IP 基础网络，其标识机制需继承互联网核心范式。类比用户通过域名访问网络服务，智能体通过请求专属的“智能体域名”，经由统一的域名映射系统解析为目标 IP 地址，确保基础互联互通。

智能体发现：伴随多智能体协同场景爆发，传统服务发现机制面临根本性挑战：无法适配智能体多元异构、动态变化的能力集。当前网络缺乏面向全域、跨不同主体智能体的统一能力注册与发现框架，导致任务驱动的精准协作效率低下。亟需构建全局智能体能力注册中心，动态维护全网智能体的实时能力图谱（包括功能接口、QoS 指标、状态负载），并基于任务需求生成最优匹配策略。

协议设计——智能体标识

智能体统一标识。智能体互联网需革新传统以人类语义为核心的 DNS 命名逻辑，构建智能体可高效解析的功能化域名体系。通过统一的智能体域名管理中心实施全周期治理，确保域名全局唯一性与智能体可操作性。可通过兼容现有网络基础设施——扩展 DNS 协议新增专属智能体资源记录类型，在维持 IP 映射基础功能的同时，承载智能体能力数据与动态状态。

智能体能力标识。超越基础寻址标识，智能体的核心价值在于其多维能力的精准标识与开放调度。能力体系可考虑结构化分层：底层“自身能力”支持管理平台对智能体进行实时监控、配置与维护，保障服务稳定性；上层“开放能力”则通过统一服务标识符抽象同类智能体能力的可调用功能接口。进一步构建实时更新的能力质量图谱，使域名解析升维为按需匹配最优资源的智能调度决策。

智能体绑定关系标识。智能体标识需支持精细化绑定关系属性，通过精细化绑定关系标识实现确权与优化调度。明确划分专属型智能体（绑定特定主体，保障高安全与优先级）与共享型智能体（公共服

务池，支持弹性分配）两类归属形态，并基于此定义差异化 SLA 与计费规则。核心在于实时维护每项开放能力的绑定状态（占用/空闲/受限）、绑定对象以及时效窗口。

协议设计——智能体发现

智能体的发现在广域环境下需要通过统一的平台进行远程协作，高效的智能体发现机制至关重要。由于智能体互联网中 DNS 解析请求将由智能体发起，为了系统的安全性，考虑对新增智能体数字身份验证流程，确保可信的 DNS 请求来源。

分级分区智能体发现：借鉴并优化传统 DNS 系统的设计理念，智能体域名解析可采用分级、分区域的分布式架构，以显著提升解析响应速度、增强系统整体稳定性和可扩展性。分区域解析依据地理位置、网络拓扑或组织边界划分解析区域，部署区域性的权威解析服务器。智能体或客户端优先向其所属区域内的本地解析器发起查询。本地解析器通常缓存高频访问的解析记录，能实现毫秒级响应；对于未缓存的请求，本地解析器再向上级或特定区域的权威服务器查询。分级与分区域的结合，共同构成了高响应、高可用、易扩展的智能体发现机制。

能力感知的动态映射：除基础标识外，解析系统可维护并动态更新智能体的详细能力画像（如处理能力、服务类型、实时负载、QoS 指标）。当接收到包含具体任务需求的解析请求时，系统能基于预设策略或机器学习模型，将智能化的域名映射到最佳可用智能体。例如，高计算强度任务可优先映射至空闲 GPU 资源丰富的智能体，而非仅

依据静态域名。这大幅提升了资源利用率和任务执行成功率。

任务驱动的优先级调度：解析系统可接入或分析智能体子任务间的复杂依赖关系、预期完成时间窗或服务等级协议（SLA）要求。据此，系统能动态区分不同解析请求的优先级。对关键路径上的任务或临近截止时间的请求给予更高处理优先级，确保其快速解析并抢占执行资源；反之，非紧急请求可适度延迟或路由至备用资源。这种基于任务上下文的优先级策略，可显著优化系统整体吞吐量和时间敏感型任务的保障能力。

4.2.2. 转发路由

功能需求

为了使能智能体的广泛互联，可在网络中部署 Agent 边界网关（AGW, Agent Gateway）。AGW 能够提供智能体注册、智能体认证、智能体发现、智能体互联等能力。AGW 相关协议包括了 Agent 与 AGW 互联协议，以及 AGW 之间互联协议等。网络中的多个 AGW 可以组成一个虚拟的智能体互联网络，为智能体互联提供连接、状态维护等服务。AGW 互联网络是一个建立在传统的互联网、云网络之上的新型互联网。

通过 AGW 互联时，AGW 一方面需要维护 Agent 到智能体互联网络的连接状态，另一方面需要维护 AGW 之间的互联，包括 Agent 之间的关联和组网状态等。

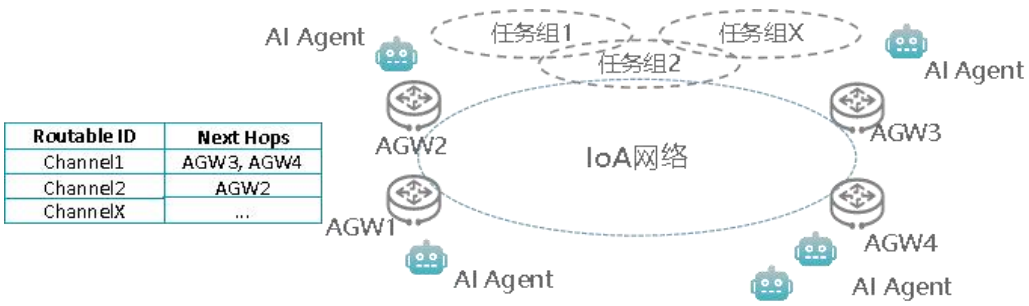

图 4-3：基于 Agent Gateway 互联的 AI Agent 网络

当智能体需要连接 AGW 与其他的智能体通信时，智能体首先需发现网络中关联的 AGW，之后需要通过 AGW 的认证和授权后，建立安全的连接。

当前智能体需与其他智能体协作时，可以直接提供一个或者多个目标智能体信息，或在智能体互联网络中搜索拥有合适能力的目标智能体，目标智能体可以通过不同的 AGW 接入。

在智能体互联网络中，涉及到两个智能体的任务组也被称为 Channel（频道），Channel 承载在多个 AGW 组成的虚拟互联网络之上。

当 Channel 包括更多的组员时，AGW 也需要能够提供任务组内的灵活通信服务。为了保障组通信的安全性，这里可以通过 Message Layer Security（MLS）来进行通信的端到端加密，具体可参考 IETF RFC 9420，RFC 9750。

协议设计

在 ID 方面，涉及智能体 ID、AGW ID 和 Channel ID。其中智能体 ID 为智能体统一标识；AGW ID 是公开的单播地址，多个 AGW 可以有相同的任播服务地址；Channel ID 与任务组的发起者相关，例如可以使用任务发起者的 ID、任务 ID 等来构建。在基于 Channel ID 进行路

由时，Channel 相关的每个 AGW 针对 Channel ID 均会维护相应路由表条目，记录各消息需要路由的目标 AGW。

在协议分层方面，AGW 互联网络需要能够提供一个会话层，从而屏蔽 MLS 的复杂操作，以及消息转发的底层实现，让上层仅仅调用发布和订阅 API，就能实现方便的通信。因此，AGW 支持处理相关的认证、加密、连接管理、错误自动恢复等。会话层协议可基于 gRPC 进行扩展，加入发布-订阅的能力，来有效的支持 AI 智能体应用的多对多的通信。

在服务发现方面，可基于分布式的 AGW 存储 AI Agent 的元数据，AGW 需支持全局唯一的内容编址，支持分布式 Hash 表（DHT）来分布式存储目录信息。

在网络管控方面，，可由一个管控节点来管理和配置 AGW，以及优化 AGW 之间的互联。管控节点需要支持 AGW 的发现、配置管理、安全策略、以及服务质量监控等。

在另外一种实现中，支持相同的互信机制和通信协议的智能体或者智能体群组也可以连接到智能体联盟的云端服务器进行灵活组网和信息交互，这时将存在迂回路由问题，但是实现相对简单。

4.2.3. 认证授权

要实现多智能体安全可信的互联协作，认证授权是重要前提，亟需为智能体的数字身份制订配套的认证授权方法，包括实现 U2A（用户与智能体）双向可信交互与 A2A（智能体与智能体）全链路可控协

作，为跨域协同提供安全底座。

功能需求

面向 U2A 和 A2A 场景，链式认证授权需聚焦**四大核心功能需求：**

一是双向身份可信需求。U2A 场景需实现用户与智能体身份互验，支持指纹、声纹等多模态认证；A2A 场景需基于 Agent 新的标识信息（如 Agent 命名服务），验证智能体身份合法性及权限来源合理性，确保协作主体可信。

二是动态权限适配需求。突破静态授权局限，实现权限与任务的“时间、范围、场景”三绑定，U2A 与 A2A 场景均需支持权限按需分配、用完回收，符合最小权限原则。

三是链式协同联动需求。认证授权流程需与智能体任务流及 Agent 命名服务的标识发现流程深度融合，形成 “Agent DNS 标识定位-U2A 授权-A2A 协作-权限回收”闭环，无需用户重复操作，保障协作连贯性。

四是全链路风险管控需求。结合 Agent DNS 的标识动态更新能力，实时监控链条异常行为，支持风险分级识别与快速响应，可阻断非法操作、同步风险信息，防止风险扩散。

协议设计

针对上述需求，链式认证与授权协议需深度协同 3.2.1 章节提到的智能体标识机制，灵活选用或扩展升级当前的技术方案，形成面向智能体互联网的认证授权方法。潜在的核心技术路径和可选方案包括：

在**身份确权与标识适配**方面，从信任模型、标识控制权、动态灵活性、兼容性等不同维度考虑，目前主要有三类技术路径可选：

一是分布式标识（DID）技术。DID 遵循去中心化的信任模型架构，依赖分布式账本完成认证。DID 可与智能体命名服务的根域名层、领域域名层架构协同，将其作为智能体标识层核心载体，遵循 W3C 规范实现自主可控的去中心化标识，元数据通过智能体命名服务的分布式存储节点同步，优势是跨域互通性强、可追溯防篡改，适配智能体之间跨组织协作，但存在存储成本高、与传统体系兼容性不足的问题，目前部分开源项目正在基于 DID 技术与智能体新型命名服务进行适配测试。

二是传统 X.509 数字证书方式。X.509 遵循中心化的信任架构，依赖层级化信任链，在智能体互联网部分场景也有较强的适用性。可考虑将 X.509 集成至智能体命名服务系统的标识管理模块，由 CA 证书授权机构签发的证书与智能体标识绑定，通过解析接口快速获取证书信息，技术成熟且与 HTTPS 等现有体系兼容，解析速度快，适合 U2A 高频交互场景，但中心化管理存在单点风险，跨域验证需通过智能体命名服务的跨域解析机制协同，存在效率问题。

三是混合模式（DID+X.509）。综合考虑两种技术方法的优劣势，通过智能体命名服务的标识映射接口关联两种标识，DID 用于跨域身份确权，X.509 证书用于域内快速认证，兼顾去中心化与兼容性，可满足渐进式落地需求。实际部署中，可根据场景对去中心化的要求灵活选择，例如政务场景下的智能体协作可通过领域域名层管理混合标

识，而完全去中心化的开源智能体生态可在分布式智能体节点仅部署DID方案。

在**双向认证与链式授权**的核心流程中，需以智能体的标识发现结果为基础，结合不同场景选择适配协议：

OAuth2.1：适配X.509证书或混合模式的域内交互场景—将解析的智能体标识（与X.509证书绑定）作为OAuth2.1的客户端ID，依托X.509的成熟加密机制强制PKCE安全验证，高效支撑U2A授权登录；跨域A2A协作时（混合模式下），需扩展Token Exchange规范，通过智能体命名服务获取协作智能体的身份标识，实现跨域权限链式传递，该方案适合需与传统系统衔接的场景。

DIDComm：专为纯DID确权路径设计——直接调用智能体命名服务的DID解析接口获取对方身份元数据，无需依赖中心化CA证书即可实现点对点加密认证与A2A全链路溯源，但目前因生态成熟度较低，开源项目正推进相关接口的深度兼容，适配去中心化要求高的跨域协作场景。

实践中可根据确权路径灵活选型，例如电商场景采用“混合模式”完成身份确权后，通过智能体命名服务定位库存智能体，再以OAuth2.1作为主协议，扩展Token Exchange实现订单智能体与库存智能体的权限传递，既利用X.509保障域内交互效率，又通过DID支撑跨域可信传递。

在**全链路风险管控**环节，需结合智能体标识状态管理能力，与认证授权流程深度融合，实现风险阻断。需通过标准化接口实时获取三

类核心数据 ——智能体标识动态数据（DID 解析记录、X.509 证书状态变更）、认证授权操作数据（OAuth2.1 令牌日志、DIDComm 交互记录）、智能体行为数据（权限申请频次、协作对象变化），确保与认证授权流程同步。

检测机制可选取硬件关联的**RATS 协议**或**基于 AI 的异常检测方法**。RATS 协议可将智能体硬件标识作为远程证明的核心凭证，验证智能体的环境完整性，适合与 DID、OAuth2.1 结合用于高安全场景，但对硬件要求较高；基于 AI 的异常检测方案可关联智能体标识动态更新日志（如智能体迁移、权限变更记录），分析 OAuth2.1 令牌调用、DID 交互等数据，识别异地高频调用、权限越界等异常，适配性强但需大量数据训练。实际应用中，可构建分级管控体系，实现全网协同防护。

4.2.4. 互联协作

互联协作是实现多个智能体之间高效协同工作的核心技术，其关键在于如何高效地发布智能体能力，并在此基础上实现多智能体之间的任务流协作。这一过程既涉及语义层面的意图理解与能力匹配，也涉及任务的协同控制，是智能体互联网从“连接导向”走向“任务导向”的关键体现。

功能需求

Agent 能力发布与任务流协作的功能需求可归纳为以下三个方面：

一是能力的语义化发布。不同 Agent 来自不同厂商，能力形式、接口标准不一致，若缺乏统一描述，协作将难以展开。因此，智能体

需要以标准化、可理解的方式向外界描述自身的能力，以便 Agent 之间可匹配。

二是任务流的动态分解与编排。复杂任务往往由多个环节组成，需要将顶层任务目标逐步拆解为可执行的子任务，并根据实时环境动态调整。任务编排要具备灵活性和自治性，这会直接影响到系统的整体效率、响应速度与鲁棒性。

三是多 Agent 的协同调度。任务协作需要保证执行过程中的时序一致性、状态同步和资源协调，子任务中任何一步延迟都会影响整体的执行效率。因此，协同调度必须具备实时性和鲁棒性，同时能适应 Agent 异构性和环境变化。

协议设计

针对上述三项核心需求，Agent 能力发布与任务流协作协议需要兼顾语义互通、任务编排和协同调度。潜在的核心技术路径和可选方案包括：

在**语义化能力描述**环节，当前主要有三类可行的技术路线。

一是基于语义网与本体建模的路线。通过 RDF/OWL、JSON-LD 等语义标准，对智能体的功能、输入输出、约束条件和服务质量进行形式化定义，并结合推理引擎实现自动匹配与组合。这一路线能够保证语义表达的一致性和逻辑的可推理性，尤其适用于医疗、工业、交通等对跨域互操作和规则合规要求较高的行业。

二是基于轻量化标准接口的路线。以 OpenAPI、AsyncAPI 等现有接口描述规范为基础，在接口说明中嵌入能力标签、元数据和 SLA 指

标，从而在保持与现有系统兼容的同时，实现能力的快速注册、检索和调用。这种方式工程实现难度低、落地速度快，特别适合企业内部和行业联盟构建统一的能力目录。

三是基于智能语义检索的路线。依托大模型语义解析与向量化表示，将自然语言能力目标转化为可计算的语义向量，并结合规则过滤和元数据校验实现能力发现与匹配。这一路线对自然语言表达有良好兼容性，能够有效支持开放生态和用户友好的交互方式，适合面向公众的智能体平台建设。

在**任务编排与工作流驱动协作**的环节，有五种可能的技术路线。

一是顺序编排。让智能体按固定顺序依次处理任务，前一个智能体的输出作为后一个智能体的输入，形成清晰的数据流管道。这种模式的优势是逻辑清晰、调试简单，但灵活性有限，任何一个环节出错都会影响整个流程。

二是并行计算——MapReduce 模式。其借鉴了分布式计算的思想，将大型任务分解为多个独立子任务，通过并行处理显著提升效率。这种模式在处理大数据量、计算密集型任务时表现出色，但需要精心设计任务分解策略，确保子任务的独立性和结果的可合并性。

三是共识模式。共识模式通过多个智能体独立处理相同问题，然后比较和整合结果来提高决策质量。其关键在于确保参与共识的智能体具有足够的多样性，避免系统性偏差被放大。

四是分层编排模式。分层编排建立了明确的管理层次，编排智能体负责任务理解、分解和调度，专业智能体负责具体执行。这种模式

能够处理复杂的跨领域问题，其挑战在于编排逻辑的复杂性和故障传播的控制。

五是制作者——检查者模式。这种模式建立了内容生成与质量控制的闭环反馈机制。制作者智能体专注于内容创建，检查者智能体负责质量评估和错误检测，通过多轮迭代逐步优化结果质量。迭代次数和退出条件的设计直接影响系统效率和最终质量的平衡。

在**多 Agent 协同调度**方面，一方面可以利用**分布式调度框架**，让各 Agent 在共享部分全局信息的基础上，通过局部决策与消息传递实现去中心化的任务分配，减少单点瓶颈；另一方面，可引入**多智能体强化学习**，使 Agent 通过长期交互学习出最优的调度策略，从而在复杂环境下实现动态优化。此外，**博弈论**与**拍卖机制**也可用于处理多 Agent 间的资源竞争与利益协调，确保调度结果公平高效。

4.3. 智能体赋能网络关键技术方向

4.3.1. 智能体赋能网络运维

传统网络管理需手动配置大量设备指令以实现业务目标，对人工经验依赖较大，意图驱动网络管理通过 LLM 等，支持将用户的自然语言意图转化为网络可以识别和执行的动作，通过自动化、智能化手段将抽象意图转化为网络配置并保障执行。智能体作为核心执行单元，凭借感知、分析、决策、执行能力，成为连接“用户意图”与“网络动作”的关键载体，大幅提升网络管理的效率与可靠性。

功能需求

智能体作为连接用户意图与网络设备的桥梁，需满足从意图解析到状态反馈的全流程支撑能力，包括以下功能需求：

一是意图接收与解析适配。智能体需支持多种接口方式接收意图指令，包括 REST API（用于云管理平台下发）、消息队列（如 Kafka，适合大规模量智能体调用并发场景）和本地配置文件（用于离线模式）。对于接收的意图指令，智能体需进行格式校验（如 JSON Schema 验证）和语义转换，将标准化意图转换为设备可理解的技术参数。

二是网络状态感知与数据采集。为了完成网络功能，智能体可以动态感知三类数据：设备资源数据（CPU / 内存利用率、端口流量、电源状态）、网络性能数据（链路时延、丢包率、抖动、路由收敛时间）和业务流量数据（应用协议分布、会话数、流量峰值）。采集方式应支持协议自适应，采集频率需可动态调整，平衡实时性与资源消耗。

三是决策分析与执行。基于感知到的任务指令和数据，智能体可以通过意图分析结果，结合知识库内的案例，将用户输入的内容转化成配置指令或者调用步骤。智能体需通过外部系统或者原子能力的调用满足用户意图。某些场景下，需要多智能体共同协作完成任务，需要确定依赖关系，并且需要智能体间的互联协议配合完成，在协议中需要对流程进行整体把控，进行会话管理等。

四是场景闭环。状态反馈与闭环修正功能保障意图执行效果。智能体需实时监控配置执行结果，可以通过设备返回码判断配置是否成功，当执行失败时，详细记录日志（包含错误类型、影响范围、建议

修复方案），进行简单分析，并将错误案例存入知识库，增强大模型能力。在意图达成度评估方面，可将采集网络状态数据与意图目标进行比对，计算偏差值并生成趋势预测。

协议设计

协议设计需满足三方面的通信需求：智能体与用户的交互、智能体间的通信、智能体与网络系统/设备的交互。

一是用户意图理解。智能体与用户交互中的意图理解协议设计，是一套定义 “用户输入 – 智能体解析” 全流程的规则体系，核心目标是消除歧义、提升解析准确性、保障交互一致性，并适配多场景、多模态的复杂需求。该协议需覆盖意图的识别、消歧、验证、更新全生命周期，同时兼顾技术可行性与用户体验。首先，在输入规范方面，定义 “可解析的用户输入”，明确智能体支持的输入类型、格式约束及预处理规则，是意图理解的基础。其次，构建结构化的意图库，明确 “意图分类”“意图要素”“场景信息” 三要素。第三，规则解析协议，明确如何将预处理后的输入与意图库匹配，完成从输入到意图的映射逻辑”，设计关键词匹配和句式匹配映射规则，辅助上下文信息与置信度阈值规则。在协议实施过程，对意图解析结果进行验证反馈模块，确保智能体解析的意图与用户真实需求一致，并能根据用户需求变化，动态更新规则，确保协议的扩展性。

二是智能体间通信。智能体间的协议框架要满足高效通信，支持任务同步、状态查询、结果确认等。协议支持流式 RPC（Streaming RPC），允许智能体持续接收进度更新（如 "配置已完成 30%"）。为确保协同

一致性，采用两阶段提交（2PC）机制：准备阶段确认所有 Agent 均具备执行条件，提交阶段同步执行配置，失败时通过固定接口统一回滚。

事件通知协议用于智能体间的实时事件传递，如智能体加入组、任务完成通知等。事件消息采用 JSON 格式，包含事件类型、时间戳、参数和签名字段，接收方通过验证签名（发送方证书公钥）确保消息真实性。协议支持事件过滤机制，智能体可订阅感兴趣的事件类型（如仅接收与自身相关的链路故障事件），减少无效消息处理开销。

三是智能体与网络的交互协议。智能体与网络之间的协议要解决智能体对网络数据的理解，在数据识别和收集上可以参考 MCP 协议，具备网络功能的一类原子能力采用标准化接口定义。

配置协议采用分层适配架构，对新型设备优先使用 NetConf 协议（RFC 6241），通过 YANG 模型（如 ietf-interfaces、ietf-qos）实现结构化配置。配置过程可分为三个阶段：获取当前配置、推送变更、提交生效，每个阶段均需设备返回确认响应。对于不支持 NetConf 的老旧设备，通过 CLI 协议适配（基于 SSHv2），将标准化配置转换为设备特定命令行，并通过正则表达式解析执行结果。

协议适配层实现统一抽象接口，提供配置、查询、监控三类通用 API，上层功能模块无需关注具体协议细节。适配层可内置协议健康检测机制，当检测到某协议通信失败（如 NetConf 连接超时），自动切换至备用协议（如 CLI），切换过程对上层透明，确保服务连续性。

4.3.2. 智能体化网络组件

随着智能体应用的发展，其感知、决策与调动能力的成熟，智能体将与网络深度融合，推动网络服务从现有的被动响应模式向主动执行跃迁，提升网络的智能化水平。按照基础网络演进的形式，智能体首先会在控制面集成，通过更高效的网络配置实现语义互通；而后转发面也会集成智能体能力，实现超高速的信息转发和跨域协同。

（1）控制面集成智能体。控制器主要执行配置功能，面向广域网络首先要进行语义配置，帮助智能体之间进行高效协作，包括基于意图的自主交互和灵活组网。同协议语义通信中，仅允许采用同种协议的智能体互传语义。要实现协议异构的智能体互联，必须引入额外的协议转换设备，使得网元之间能够利用深度神经网络的多层结构和层次化抽象机制与信息处理的层次化机制共通，为从根本上解决通信网络中跨系统、跨协议、跨网络不兼容难互通问题提供新思路。

（2）数据面集成智能体。在转发设备集成智能体，一方面可以方便转发设备与网络管控节点的灵活通信，另一方面也可以更方便地使能转发设备与转发设备之间的多维感知、流量调优和任务协同，提升网络的运维效率和转发效率。面向算网智一体化演进，可以配合算力路由、在网计算等算网融合技术，在网络入口节点通过用户需求和算网状态的综合感知优化用户流量调度，避免网络资源和算力资源的局部过载，提升用户体验；还可以在网内集成算力能力，使能“转发及计算”的新型算网一体模式，从算网全局进行任务优化。

4.4. 协议栈构想

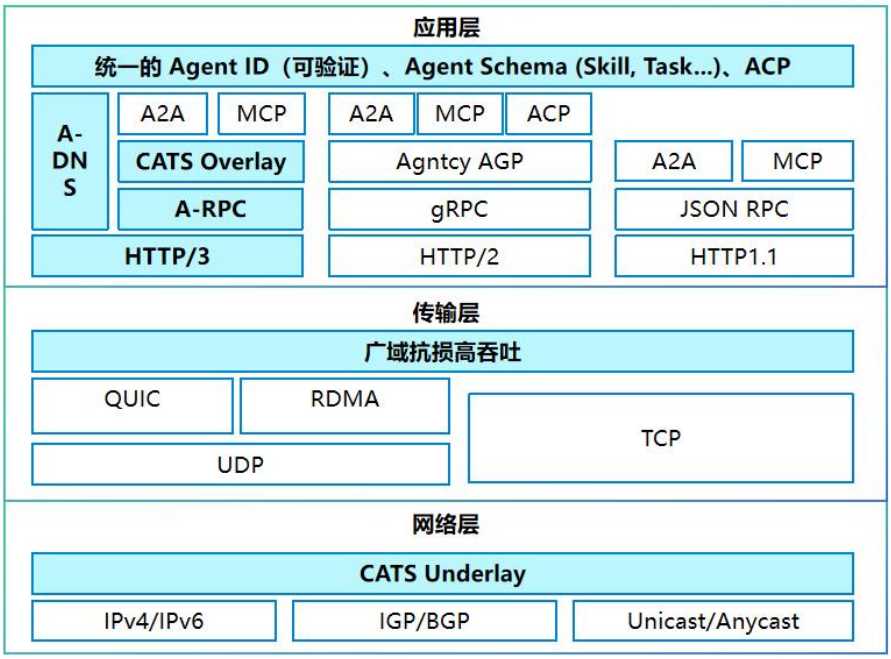

图 4-4 智能体互联网协议栈示意图

图 4-4 协议栈的构想图里面，基础网络层包括传统的这种 IP 转发，以及路由控制技术，传输层包括 TCP、QUIC、RDMA 等面向多模态业务的各类数据传输协议。应用层，也就是前文提到的面向智能体互联和任务协作的“新 5 层”，包括了业界现在主流的智能体之间的互联协议，如 A2A、ACP、ANP 等，以及智能体和工具之间调用的协议 MCP 等等。前文还提到的将来智能体之间的互联还包括可能出现全新的标识体系，如 A-DNS，与智能体互联相匹配的一些进程调用协议，以及智能体之间的 overlay 路由协议.在此之上的智能体任务协作层包括智能体之间之间的任务、能力发布协议、认证授权协议等。

协议栈总体归纳了业界已有的技术路线，以及本白皮书提到的可能存在的其他候选协议，未来将持续进行技术路线的收敛和演进。

5. 发展倡议

智能体互联网作为新质互联网的代表，正开启互联网革命的新浪潮。本白皮书系统勾勒了智能体互联网的目标愿景、架构设想与关键技术方向，为行业发展提供了参考。面向新阶段，需要持续携手共进，共同迈向智能体互联网的伟大目标：

一是进一步推进智能体应用纵深发展，强化业务需求牵引。以产业痛点为导向，推动智能体在工业制造、政务服务、智慧医疗等重点领域的场景化落地，通过试点示范凝练典型需求，反哺技术迭代，形成良性循环，为智能体互联网演进指明方向。

二是进一步收敛明确智能体互联网技术发展路径，加快关键技术攻关。聚焦标识发现、转发路由、认证授权等核心技术方向，收敛碎片化技术探索，形成统一技术路线图。依托产学研用协同创新平台，重点突破跨域智能体发现效率、链式授权安全性、多智能体系统协作调度等瓶颈，构建自主可控的技术体系，夯实产业发展根基。

三是进一步凝聚产业合力开展国际国内标准化布局。积极参与IETF、ITU-T、3GPP、CCSA 等国际国内组织相关工作。联合企业、科研机构、行业协会组建标准化工作组，加快智能体互联网总体架构、核心协议、接口规范等标准制定，确保技术兼容性与产业协同性，主动输出技术方案与标准提案，推动形成全球公认的架构体系与协议规范，降低国际协作壁垒。

智能体互联网的发展需要各方协同发力。期待政府、企业、科研

机构携手合作，以需求为锚、以技术为基、以标准为纲，共同推动智能体互联网规模化发展，为数字经济高质量发展注入强劲动力。

缩略语列表

缩略语	英文全称	中文全称
A2A	Agent 2Agent	智能体到智能体
MCP	Model Context Protocol	模型上下文协议
ANP	Agent Network Protocol	智能体网络协议
U2A	User to Agent	用户到智能体
UPF	User Plane Function	用户面功能
DID	Decentralized Identifiers	分布式标识
OAuth	Open Authorization	开放授权
AGW	Agent Gateway	智能体边界网关
IoA	Internet of Agents	智能体互联网
QoS	Quality of Service	服务质量

引用

1. Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", RFC 9420, DOI 10.17487/RFC9420, July 2023, <https://www.rfc-editor.org/rfc/rfc9420>.

2. Beurdouche, B., Rescorla, E., Omara, E., Inguva, S., and A. Duric, "The Messaging Layer Security (MLS) Architecture", RFC 9750, DOI 10.17487/RFC9750, April 2025, <https://www.rfc-editor.org/rfc/rfc9750>

3. Maymounkov, P. and D. Mazieres, "Kademlia: A peer-to-peer information system based on the xor metric", IPTPS '01 , 2001.