XXXX

面向企业多智能体协同的专网架构及关键技术研究

韩政鑫，何涛，韩梦瑶，庞冉，曹畅，唐雄燕
（中国联合网络通信有限公司研究院，北京 100048）

摘　要：人工智能正从以大模型为主导的阶段向自主协同的智能体方向演进。针对企业数字化转型中多智能体规模化协同面临的核心挑战，聚焦企业及园区应用场景，探索性地提出以“智能体网关”为核心枢纽的专网架构，研究涵盖智能体标识与注册、能力发现、高效通信以及安全协同的关键技术体系，并创新性地提出基于IPv6地址的智能体标识与语义路由机制。该架构依托智能体网关，通过网络层与应用层能力协同，实现异构智能体的可信接入、能力发现与高效协作，为企业及园区级智能体协同提供技术参考与实践路径。

关键词：智能体；企业专网；智能体网关；多智能体协同
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.

Research on Private Network Architecture and Key Technologies for Enterprise Multi-Agents Collaboration

HAN Zhengxin, HE Tao, HAN Mengyao, PANG Ran, CAO Chang, TANG Xiongyan
China Unicom Research Institute, Beijing 100048, China

Abstract: Artificial intelligence (AI) is evolving from a stage dominated by large language models (LLMs) towards autonomously collaborative AI agents. To address the core challenges of large-scale multi-agent collaboration in enterprise digital transformation, focusing on enterprise and park application scenarios, an AI agent private network architecture with "AI agent gateway" as the core hub was exploratorily proposed. The key technology system covering AI agent identification and registration, capability discovery, efficient communication, and secure collaboration was studied, and an AI agent identification and semantic routing mechanism based on IPv6 addresses was innovatively proposed. Relying on the AI agent gateway, the architecture realizes trusted access, capability discovery, and efficient collaboration of heterogeneous AI agents through the collaboration between network layer and application layer capabilities, providing technical reference and practical paths for enterprise-level multi-agent collaboration.

Key words: AI agent, enterprise private network, agent gateway, multi-agent collaboration

收稿日期：XXXX−XX−XX；修回日期：XXXX−XX−XX

1 引言

人工智能（Artificial Intelligence, AI）正经历从“工具辅助”向“自主协作”的范式演进，以ChatGPT、Deepseek为代表的大语言模型（Large Language Model, LLM）开启了生成式AI的新纪元，而基于LLM的智能体（Artificial Intelligence Agent, AI Agent）通过融合记忆管理、任务规划、工具调用与自主行动能力[1]，标志着AI应用进入“自主决策”新阶段。与传统软件程序不同，智能体具备环境感知、意图理解、任务分解与持续学习的特性，能够自主完成复杂的任务，正在成为重塑企业数字化转型的关键使能技术。

随着智能体在企业研发设计、生产制造、运营管理等环节的深入渗透，单一智能体的能力已难以满足复杂业务场景的多样化需求，多智能体协同成为突破单体智能体局限、实现“群体智能”的必然趋势[2]。然而，现有企业网络架构主要面向“人—机”或“设备—云”的连接设计，网络承载能力、集中式服务发现机制以及边界安全防护策略已难以适配由AI驱动的新兴业务需求。

智能体的规模化部署及动态自主的协作模式对现有企业网络提出了新的挑战[3]：通信行为呈现高频率、强动态、大上行特征，对网络灵活性、带宽及服务质量提出了更高要求；异构智能体采用多样化的通信协议与数据格式，缺乏统一的身份标识与能力发现机制；智能体间的跨域协作对数据安全、行为可信与全局可控构成了严峻考验。

针对上述挑战，本文探索性提出基于智能体网关的企业智能体专网架构，系统研究专网场景下的智能体标识与注册、能力发现、高效通信以及安全协同等关键技术，实现企业、园区异构智能体的统一接入、可信互联与高效协同，构建面向智能体互联的新型企业专网服务体系，为智能体的规模化应用与协同提供基础。后续将通过原型测试与试点应用验证方案效果，推动技术从研究探索向工程实践落地。

本文后续章节安排如下：第2章综述国内外智能体网络相关研究进展；第3章分析企业智能体专网场景及其对网络的共性需求；第4章提出基于智能体网关的企业智能体专网架构设计；第5章详细论述智能体专网与网关的关键技术，提出基于网络层IPv6地址的智能体注册与能力发现机制；第6章总结全文并展望未来研究方向。

2 国内外研究现状

2.1 智能体通信协议

当前智能体通信协议呈现多协议并存的格局，主要包括模型上下文协议（Model Context Protocol, MCP）、智能体间协议（Agent-to-Agent Protocol, A2A）和智能体网络协议（Agent Network Protocol, ANP）等[2][3]。MCP由Anthropic公司于2024年开源，聚焦智能体与外部工具、数据源之间的连接，采用客户端-服务器架构，是智能体调用外部资源的事实标准。A2A由Google联合50余家企业于2025年推出，基于HTTP、SSE等Web标准构建智能体间点对点通信能力，通过Agent Card机制实现智能体能力的发现，适配企业级智能体协作场景，与MCP形成互补。ANP由国内技术团队主导于2025年开源，采用去中心化对等网络架构，依托万维网联盟（World Wide Web Consortium, W3C）去中心化标识符（Decentralized Identifier, DID）实现智能体可信互联，适用于开放互联网协作场景。表1对三种主流协议进行了对比分析。

2.2 智能体互联网架构与网关技术

研究机构、运营商与设备商积极布局智能体互联网（Internet of Agents, IOA）架构研究，发布多项白皮书与研究报告，为智能体组网提供了框架支撑。中国联通研究院发布的《智能体互联

表 1　主流智能体通信协议对比

协议名称	发起方	核心定位	架构模式	生态	特点
MCP	Anthropic（美国）	智能体与工具标准连接	客户端-服务器	1100+项目，相关开发 SDK 比较完善	成熟度高，易落地
A2A	Google（美国）	企业级智能体间协作	混合式（支持中心化协调）	50 余家全球科技企业支持，兼容主流框架	支持度高，适合复杂任务，与 MCP 互补
ANP	ANP 开源社区（中国）	去中心化智能体互联协作	P2P（点对点）	国内阿里、字节等众多科技企业开发者参与	去中心化设计,安全性强，生态建设持续增强

网白皮书》[4]系统阐述了智能体原生网络架构与关键技术，提出智能体专网作为 IOA 在垂直行业的落地载体，具有场景适配性强、短期可落地的优势。华为发布《智能体互联网架构与关键技术研究报告》，提出涵盖物理网络层、智能体连接层、管控层及应用层的 IOA 四层架构，智能体网关作为连接层的核心锚点是 IOA 的关键组件[5]。

产业界方面，智能体网关从概念逐步进入产品化。 国际层面，开源组织 Linux 基金会纳入 Agent Gateway 等项目，原生支持 A2A、MCP 等主流协议。国内方面，科研院所、设备商提出语义路由中间件及智能体注册方案，研发网关原型机[6]；大型互联网企业推进 API 网关智能化升级，推出 AI 网关实现存量 API 向 MCP 协议转换，适配金融、云部署等场景；中小型科技企业发布智能体物联网关，实现多场景智能调度与数据处理。现有方案多侧重于应用层协议适配，网络层与应用层的深度融合仍是亟待突破的难题。

2.3　智能体互联网标准进展

智能体相关技术成为全球热点，国内外主要标准组织纷纷启动智能体网络相关研究：第三代合作伙伴计划（3rd Generation Partnership Project, 3GPP）在 6G 研究（TR 22.870）中提出了支持第三方智能体可信接入、安全标识与跨域协作的业务需求。互联网工程任务组（Internet Engineering Task Force, IETF）已成为智能体通信协议标准化主战场，围绕智能体协议、智能体与网络的双向赋能、企业智能体组网等议题，已组织多场专题研讨会，并涌现大量个人草案。国际电信联盟电信标准化部门第 13 研究组（International Telecommunication Union - Telecommunication Standardization Sector, Study Group 13, ITU-T SG13）启动了智能体通信网络需求、术语及路线图等研究项目，逐步明确标准方向。中国通信标准化协会（China Communications Standards Association, CCSA）已成立智能体网络子组，推进智能体协同架构、标识注册及承载网增强等关键技术研究，已有部分在研标准。总体来看，当前智能体网络仍处于场景梳理、需求探讨与框架构建的早期阶段，多以研究报告或草案形式呈现，尚未形成标准体系。

3　企业智能体专网场景与需求分析

3.1　应用场景

在企业环境中，多智能体需协作执行复杂任务。依据企业智能体业务的组织形态、协同范围与网络边界特征[7]，将其应用场景可划分为以下三类。

（1）园区内网协作：智能体部署在单一企业或园区的内网，网络时延低、质量稳定。智能体数量相对有限，处于同一信任域内，经过统一认证与管理，对通信的实时性和可靠性要求较高。典型应用包括多机器人协同作业、智能排产调度、自适应工艺优化等。

（2）跨园区广域协作：同一企业的不同园区、分支机构或合作企业之间的智能体，通过企

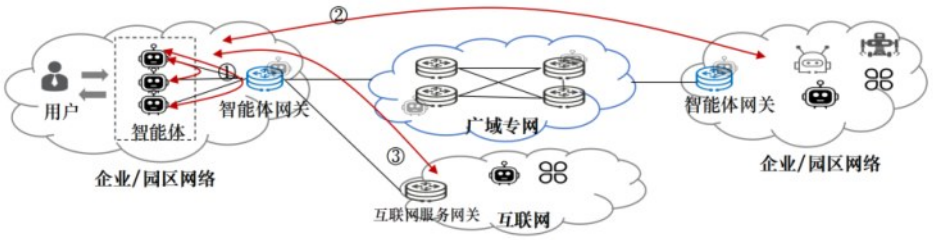

图1　企业/园区智能体协作场景

业专网或专线实现跨域协同。智能体来自不同可信域，网络链路相对复杂，时延和抖动更易波动，对网络服务质量、跨域服务发现及策略一致性提出了更高的要求。典型应用包括跨园区生产协同、供应链资源调配以及跨区域运维调度等。

（3）受控互联网协作：对于部分业务，企业/园区内部智能体以受控方式访问公共互联网中的外部智能体或服务。该场景环境不确定性高，外部智能体身份可信度未知，对接入控制、权限管理以及数据隔离具有更严苛要求。典型应用包括调用第三方AI服务、参与开放式生态协作等。

3.2　企业网络需求分析

相较于面向公众的开放化智能体应用，企业级智能体承载着核心生产运营任务，智能体根据任务动态组建临时协作网络，并在任务完成后释放资源。企业网络需在传统能力基础上，进一步满足以下新需求：

（1）异构互联与资源协同：企业内往往并存多智能体平台与通信协议（如A2A、MCP、ANP）等，需通过协议转换与语义适配能力实现异构智能体无缝通信，并协同调度网络与智能体所需的计算、存储等资源，保障任务的执行效率。

（2）分层通信与能力发现：多智能体的点对点通信压力大，需通过统一接入与汇聚网关，支持分层分级通信及能力通告，实现企业内及跨域场景下智能体快速发现与高效协同。

（3）差异化服务质量保障：智能体任务需求多样，不同任务对实时性、可靠性、带宽等要求差异显著。企业网络需融合语义理解，具备应用感知与灵活编排能力，实现异构流量的精准识别与分级调度，按需保障业务服务水平协议（Service Level Agreement, SLA）。

（4）安全与可控：企业数据资产敏感度高，智能体具备自主决策能力易引发安全隐患。企业网络需支持智能体的身份认证、动态授权与行为审计，实现从接入到交互的全流程可信管控。

（5）轻量与智能运维：企业需要“智能体友好型”轻量化、服务化、易维护的网络，具备可监测、可视化、自动化运维能力及平滑演进路径，屏蔽底层网络复杂度，支撑智能体的规模化应用与长期扩展。

4　企业智能体专网架构设计

4.1　智能体专网架构

结合企业智能体协作对异构互联、能力发现、安全可信等核心网络需求，依托企业/园区现有网络基础设施资源[8]，本文探索性设计了分层解耦、协同联动的企业智能体专网四层架构。该架构自上而下分为应用服务层、管控调度层、互联通信层与物理资源层，如图2所示，各层级通过标准化接口协同联动，形成“应用支撑-管控赋能-连接保障-资源底座”的架构体系。遵循"集中式管控、去中心化服务"理念，在保障全局策略一致性的同时，支持智能体按需动态组建协作网络，实现企业智能体在园区内网、跨广域专网

及受控互联网场景下的安全、高效、灵活协作，为企业级智能体协同提供全流程网络支撑。

（1）应用服务层：作为智能体专网的应用支撑核心，提供智能体全生命周期管理能力。核心功能模块包括智能体注册认证、智能体发现、智能体信息管理及权限管理。通过构建统一的服务目录与身份标识体系，该层实现企业内办公、流程优化、产线作业等多类型智能体的标准化纳管，为各类智能体应用提供服务化能力支撑。

（2）管控调度层：承担智能体协同的全局任务编排与资源优化调度职能。核心功能涵盖任务拆解、任务编排、语义路由、策略控制及全局可视监控。通过融合业务语义理解与网络状态感知，能够将复杂的业务意图转化为可执行的智能体资源调度与网络策略指令，实现复杂任务的多智能体协同分解、路径规划及动态策略调整，确保跨域协作任务的高效执行与SLA保障。

（3）互联通信层：是企业智能体专网实现智能体互联互通的关键桥梁，智能体网关为该层的核心组成元素。该层功能包括智能体连接相关能力与网络通信相关能力两大维度。智能体网关通过协议转换实现主流智能体通信协议的适配转换，借助标识解析与路由协议扩展支撑智能体的跨域发现与信息通告，通过网络能力封装将底层网络资源转化为智能体可感知调用的通信服务，同时通过安全防护与性能保障机制，确保数据传输的可信性与稳定性，为智能体间交互提供可靠支撑。

（4）物理资源层：作为企业智能体专网的基础设施底座，涵盖计算、存储与承载网络等核心资源，为专网提供稳定的硬件资源与传输链路。承载网络由企业内网（现场网、办公网、园区网）与企业外网（广域网专线及虚拟专网）构成，支持以太网、Wi-Fi、5G、PON、工业总线

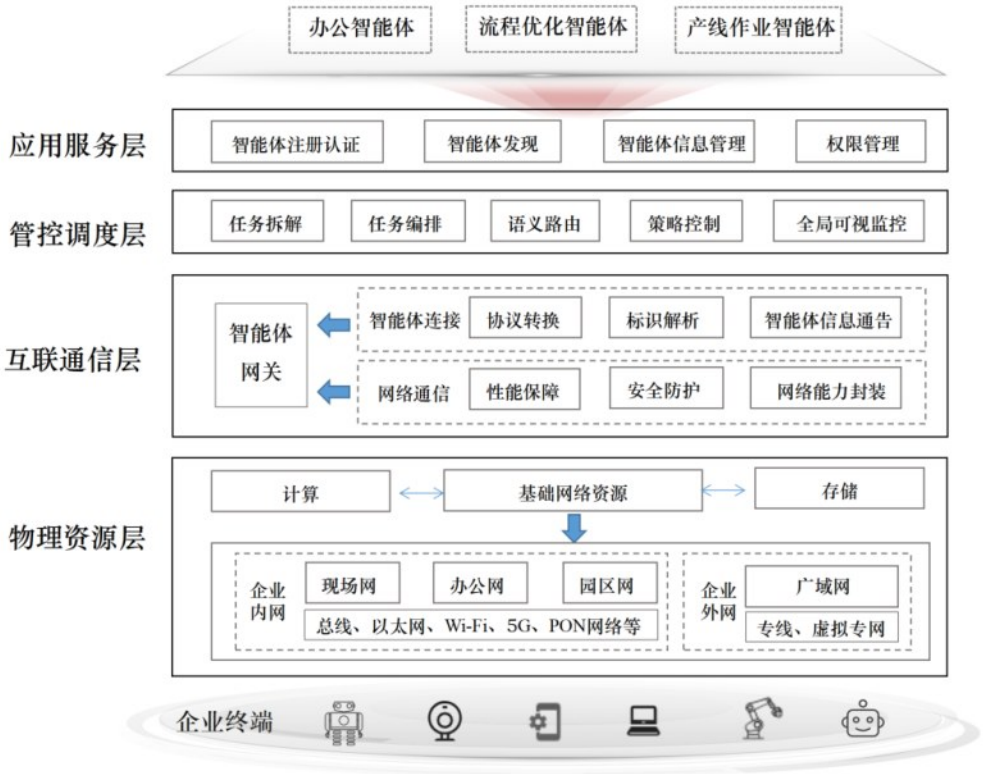

图2　企业智能体专网架构

等多种网络接入与传输技术[9][10]。该层通过资源的弹性调度与策略执行为智能体通信提供确定性传输能力、弹性算力供给及分布式存储保障，满足企业级应用对低时延、高可靠与资源隔离的承载需求。

4.2 智能体网关的定位与功能

智能体网关作为企业智能体专网的核心枢纽，部署于企业/园区出口位置，兼具通信网关的可靠传输能力与智能体的认知决策特性，承担着连接中枢、策略执行与安全守卫的角色，实现智能体间的可信接入、高效通信与协同作业。

如图3所示，在企业智能体专网方案中，基于智能体网关构建overlay的智能体专网平面。智能体网关与企业/园区内部交换机、路由器、专线等网络设备互联，通过北向接口与注册中心（新型DNS）、编排控制器、智能体应用服务平台协同交互。智能体在接入网络时向所在园区的智能体网关发起注册请求，由网关完成身份验证，将智能体元数据上报至注册中心，并承担后续通信请求的权限验证与转发控制。对于同一园区内的智能体通信，通过智能体网关认证建立连接后，后续可直接点对点直连通信无需绕行网关转发。对于跨园区智能体通信，须通过各域智能体网关进行互通，实现跨域智能体能力发现、状态同步与路由转发。

智能体网关核心功能体现在以下四方面：

（1）开放网络能力，构建“通信智能体”。将核心网络功能抽象并封装为智能体可调用的服务或工具，使其易于集成至智能体的工作流与决策逻辑中。智能体接入网关，相当于接入了一个“通信智能体”，能够屏蔽底层网络复杂度。

（2）协议转换适配，支撑异构跨域互联。作为智能体间的“协议转换桥梁”，实现A2A、ANP、MCP等主流通信协议及数据格式的适配转换，支持多类型网络接入方式（包括企业Wi-Fi、以太网、光纤等），跨网关智能体信息同步与路由表生成，实现企业跨园区智能体服务的一跳接入与快速发现。

（3）聚合工具资源，拓展应用边界。通过智能体网关可接入“可信工具与应用市场”，使企业能够安全调用丰富的生产业务工具、数据库等资源，通过资源聚合扩展智能体能力边界，适配多样化企业场景。

（4）构筑安全管控，保障可信互联。提供基于智能体身份标识的接入认证、访问控制、生命周期行为审计等安全功能，集成防火墙能力，实

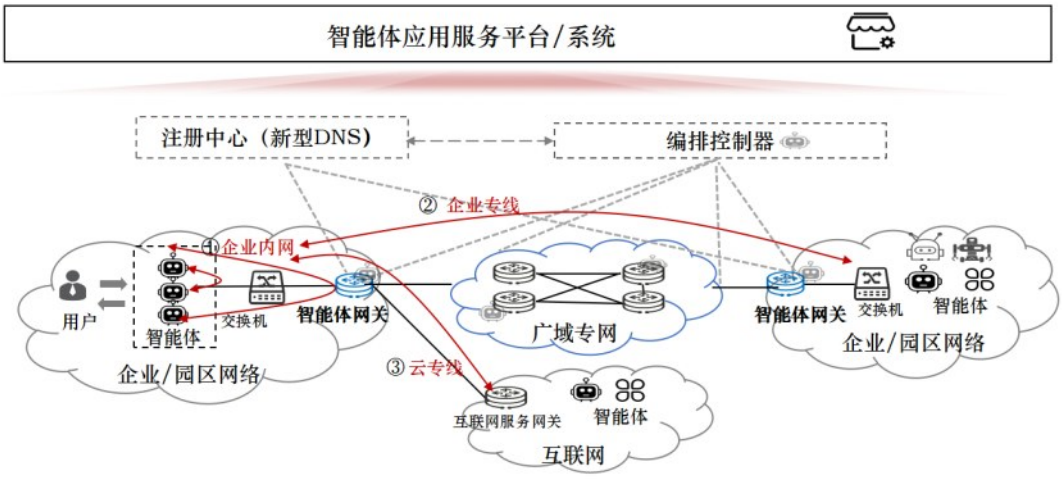

图3 企业智能体专网和网关互联方案

现企业智能体互联过程的可信可控，有效防范未授权访问及数据泄露风险。

5　企业智能体专网和网关关键技术

5.1　智能体的标识与注册

智能体标识与注册是实现智能体互联互通的基础环节。在智能体互联网场景下，智能体数量呈海量级增长、类型高度异构，且跨域交互频繁，传统标识与注册机制面临兼容性差、语义缺失、注册效率低等问题。当前的主流技术包括：基于增强型域名系统（Domain Name System, DNS）的标识方案[11]，基于IPv6的专用标识方案[12]，以及基于区块链与DID的去中心化身份管理方案[13]。

本文重点关注适用于企业智能体专网基于IPv6的智能体标识，提出一种基于IPv6地址的智能体语义标识方案，将智能体的类型、区域、能力摘要和实例标识统一编码到标准128位IPv6全球单播地址中，实现“地址即语义指纹”的标识体系，为智能体的发现、寻址和路由提供统一的标识基础。

表2　智能体IPv6语义地址字段结构

字段名称	长度	字段说明
Global Prefix	48位	智能体所属网络域/运营商前缀
Agent Type ID	8位	智能体类型标识（LLM/视觉/代码等）
Zone/Loc ID	8位	部署区域标识（端/边/云）
Capability Hash	32位	能力摘要哈希值
Instance ID	32位	实例唯一标识（含冲突计数位）

智能体IPv6语义地址采用分层字段编码，如表2所示。Global Prefix标识智能体所属的网络域或运营商，兼容现有IPv6前缀分配策略。Agent Type ID表示智能体类型或服务大类，如通用大模型（Large Language Model, LLM）、法律咨询智能体、视觉理解智能体、代码生成智能体等，支持256种类型定义。Zone/Loc ID表示智能体所在逻辑区域或部署层级，如端侧、园区边缘、城域边缘、中心云等，支持256种区域划分。Capability Hash对智能体静态能力集（模型家族、参数规模、多模态能力、工具列表等）进行规范化排序后经哈希运算得到能力摘要。Instance ID用于同一类型智能体实例的区分标识。

智能体注册采用“能力描述采集—字段映射—地址生成—注册发布”四步流程，如图3所示。在性能方面，后续将通过实验对智能体注册响应时延、并发处理能力、智能体标识管理规模等关键指标开展针对性验证与分析。

（1）智能体向注册中心上报自身能力描述，包括服务类型、模型配置、部署区域、支持模态、工具列表等元数据。

（2）注册中心根据服务类型映射到预定义的Agent Type ID，根据部署位置映射到Zone/Loc ID，并对能力特征进行规范化排序后计算Capability Hash，确保相同能力产生相同的哈希值。

（3）在确定前缀下分配唯一的Instance ID，形成完整128位IPv6语义地址，并进行重复地址检测。（4）将该地址与智能体实例绑定，通过智能体信息路由协议（Agent Information Routing Protocol, AIRP), 基于内部网关协议（Interior Gateway Protocol, IGP）/边界网关协议（Border Gateway Protocol, BGP）扩展,通告到网络中的智能体网关。

5.2　智能体能力发现

智能体能力发现是指智能体在一个网络环境中自动发布、发现并理解其他智能体所提供的功

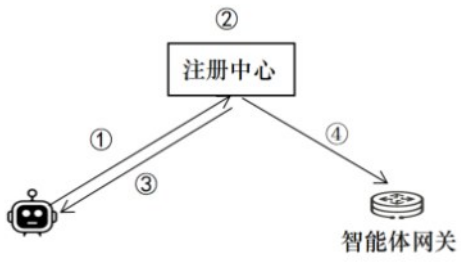

图4　智能体注册流程图

能与服务。它是实现异构智能体协同的关键环节，旨在解决“如何找到具备特定能力的智能体”这一核心问题。当前主要技术路径有基于目录服务的集中式发现[14]和基于语义与本体的增强发现[15]两类技术方案。

本文提出基于IPv6语义地址和智能体感知选项（Agent Awareness Option, AAO）的智能体语义路由机制，在数据面实现智能体的在网搜寻与能力匹配，支持网络层对智能体语义的感知和处理。AAO可以采用“类型-长度-值”（Type-Length-Value, TLV）格式封装在IPv6扩展头中，详细定义如表3所示。

表3　AAO（智能体感知选项）字段结构

字段名称	长度	说明
Option Type	8位	TLV类型标识
Opt Data Len	8位	TLV数据长度
Semantic Action	16位	语义动作：FIND/EXEC/SYNC
Agent Semantic ID	128位	智能体语义标识
Compute Cost	16位	预估算力需求
Load Status	8位	当前负载水位（0-100%）
Zone/Loc Info	8位	区域信息（端/边/云）
Context Vector Hash	可变	上下文布隆过滤器摘要

当用户发起智能体搜寻请求时，AAO中的Semantic Action置为FIND（表示搜寻），目的IPv6地址配合填写为语义任播地址。智能体网关接收到FIND报文后，完成智能体发现。流程分为以下四个步骤：

（1）智能体网关解析AAO，提取Agent Semantic ID、Compute Cost等信息；

（2）在本地地址族转换（Address Family Translation, AFT）中查找符合语义条件的智能体候选集；

（3）计算综合代价（网络延迟+算力负载+能力匹配度），选择最优智能体实例；

（4）将报文目的地址由任播地址改写为选中的智能体单播地址，完成智能体的精确定位。

智能体能力发现与智能体转发表（AFT）深度协同，AFT中维护智能体实例的多维度信息，通过FIND动作触发AFT查询，实现从语义需求到具体实例的动态映射。在性能方面，该方案可有效提升智能体能力发现与匹配的效率和准确性，实现智能体注册/注销后AFT表项的快速更新，后续实验将对能力发现、能力匹配、AFT查询及表项更新时间等相关指标进行验证。

5.3　智能体管控调度

随着智能体技术的快速发展，未来智能体将得到广泛部署并用于实现任务的自动化处理，智能体的数量将呈指数级增长。在企业园区专网中，智能体不仅需要根据任务需求执行计算、感知与决策任务，还需与其他智能体协同工作，形成一个高效的智能体网络。智能体管控调度机制的创新与优化将是提升企业系统效能的刚需。

基于对企业智能体应用场景的分析，单园区内智能体调度侧重于资源效率与实时控制，跨园区的协同调度则需解决域间信任、策略协同与状态同步问题。通过引入具备能力匹配、动态调度、资源优化特点的集中式管控调度系统，将为企业、园区智能体协作提供高效、可靠的任务执行保障。智能体管控调度系统由以下几个关键模块组成：

（1）能力匹配度计算：采用语义匹配算法，根据任务的需求与智能体的能力描述（如服务类型、能力摘要等）进行匹配，确保任务能够高效地分配给具有最佳能力的智能体。

（2）智能体状态监测：系统实时监控智能体的负载、队列长度、健康状态等指标，并进行可视化呈现。当某一智能体出现故障或负载过高时，调度系统能够自动触发故障转移或负载均衡操作。

（3）安全与合规保障：在调度过程中，考虑到任务对安全合规的需求，调度系统能够评估智能体是否符合安全等级要求。

（4）多属性决策支持：通过多维度的综合评分方法（能力匹配度、实时状态、网络质量等），系统能够选择最优的智能体组合进行任务执行。

5.4　网络能力开放与服务保障

为支撑企业智能体高效协同，网络需从被动管道转型为主动、可调用的服务。通过标准化、模块化的方式，将底层网络资源与功能进行抽象、封装与开放，使网络能够被智能体及上层业务灵活调用与编排。同时，网络须具备感知业务意图的能力，将业务意图自动转化为网络策略与服务，提供满足业务差异化需求的性能保障。

（1）网络功能封装与能力开放：基于软件定义网络（Software Defined Networking, SDN）技术，通过SDN控制器对底层网络资源进行统一抽象，并向上层系统提供网络能力开放接口[16]。对内预编排原子能力，对路由、策略、安全等核心网络功能进行封装；对外提供标准化调用接口，实现以可插拔工具或智能体的形式对外提供服务；使企业智能体能够根据业务需求灵活调度网络资源与服务。

（2）意图驱动网络服务：通过段路由（Segment Routing over IPv6, SRv6）、应用感知（Application-aware Networking, APN）、LLM等技术，实现从业务意图到网络策略的智能映射。企业用户通过自然语言描述表达网络需求，系统自动将其转换为具体的网络配置与路径策略，并通过网关等设备实现端到端的业务保障。

（3）服务质量保障（Quality of Service, QoS）：企业智能体间通信包括实时控制指令、媒体流、模型更新等多模态数据，其带宽、时延、抖动、丢包率等需求各不相同。通过网络切片、流量工程、优先级调度等技术，为不同业务提供差异化的SLA保障。此外，通过实时监测网络状态与业务性能指标，系统可开展策略动态调整，确保关键智能体业务始终获得稳定、优质的网络体验。

5.5　安全与隐私保护

企业智能体专网的安全可信保障涵盖接入安全、通信安全、行为安全和数据安全四个维度。围绕智能体与操作人员两类主体构建分层统一、协同联动的安全防护机制。

接入安全采用多因素认证机制，智能体与操作人员的身份认证为两套独立但联动的体系。智能体接入时需提供数字身份凭证、能力描述证明和行为基线报告，网关完成身份验证、能力审计和可信评估，通过后方可接入。操作人员依托企业统一身份系统完成认证。两类认证在网关侧联动，确保"人-机"操作可追溯。

智能体通信安全依托端到端加密技术与零信任机制。对于企业跨域场景下智能体之间的通信建立加密隧道，实现传输过程的安全保护。实施最小权限访问控制，智能体仅能获得完成任务所需的最小数据访问权限，所有通信行为（含智能体间、操作人员与智能体交互）均被记录至不可篡改的审计日志中，支持事后追溯[17]。

行为安全通过异常检测和态势感知技术防范恶意智能体。建立智能体行为基线模型，监测偏离基线的异常行为；同步针对操作人员建立操作行为审计基线，结合企业网络跨域威胁情报共享与动态权限调整，有效防御恶意行为。

数据安全层采用隐私计算技术保护敏感信息。通过同态加密、安全多方计算、差分隐私等隐私计算技术，实现“数据可用不可见”。在数据流转过程中实施分级分类保护，敏感数据自动加密和脱敏。建立数据主权管理机制，确保数据所有者对数据使用的知情权和控制权[18]。

6　结语

本文聚焦企业级智能体规模化协同中的网络互连与协同问题，系统梳理了智能体网络领域的研究进展与产业实践，深入分析了企业场景下智能体应用的网络需求，探索性提出了适配企业场

景的智能体专网架构及配套关键技术体系。在技术层面，本文创新性地提出了基于IPv6地址的智能体标识方案，以及基于语义路由的智能体能力发现机制，通过网络层与应用层能力的协同，为企业构建智能体协同网络提供理论与技术支持。企业智能体专网的构建宜遵循“由内而外、分阶段演进”的路径：第一阶段，聚焦在单一园区场景，实现智能体协同与网络自智的核心能力闭环验证；第二阶段，逐步实现跨园区、跨组织的智能体协同，突破域间信任与策略协同难题；第三阶段，构建开放生态，支持全域智能体的按需协作与自主运营。在此过程中，电信运营商可充分发挥网络覆盖、技术积累与可信中立的核心优势，通过提供企业智能体专线、组网与专网运维等服务，赋能垂直行业智能化转型，拓展新型业务生态。

作为IOA在垂直行业的关键落地形态，企业智能体专网的技术成熟与生态完善仍需产学研各方协同探索。本文研究目前处于前瞻性探索与方案设计阶段，后续研究将聚焦于智能体网关的研发，开展跨域协同机制的实践验证与性能指标测试，根据测试结果优化架构与技术方案，并积极推动相关技术标准的制定与统一，以支撑智能体从单体能力向群体智能的持续演进。

参考文献：

[1] 段晓东, 孙滔, 陆璐, 等. 智能体互联网：概念、架构及关键技术[J]. 智能科学与技术学报, 2024, 6(2): 165-176.
DUAN X D, SUN T, LU L, et al. Internet of agents: conception, architecture and key technologies[J]. Journal of Intelligent Science and Technology, 2024, 6(2): 165-176.

[2] ADIMULAM A, GUPTA R, KUMAR S. The Orchestration of Multi-Agent Systems: Architectures, Protocols, and Enterprise Adoption[J/OL]. arXiv: 2601.13671, 2026.

[3] GUO C Y, DUAN X D, SUN T, et al. AI Agent Communication from Internet Architecture Perspective: Challenges and Opportunities[J/OL]. arXiv: 2509.02317, 2025.

[4] 中国联合网络通信有限公司研究院, 下一代互联网宽带业务应用国家工程研究中心. 中国联通智能体互联网白皮书[M]. 北京: 中国联合网络通信有限公司, 2025.
CHINA UNICOM RESEARCH INSTITUTE, NATIONAL ENGINEERING RESEARCH CENTER FOR NEXT GENERATION INTERNET BROADBAND BUSINESS APPLICATION. China Unicom Agent Internet White Paper [M]. Beijing: China Unicom Co., Ltd., 2025.

[5] 华为. 智能体互联网架构与关键技术研究报告[M]. 深圳: 华为技术有限公司, 2025.
HUAWEI. Research Report on Agent Internet Architecture and Key Technologies[M]. Shenzhen: Huawei Technologies Co., Ltd., 2025.

[6] 全球固定网络创新联盟. AI Agent通信网关技术研究报告[M]. 深圳: 全球固定网络创新联盟, 2025.
WORLD FIXED NETWORK INNOVATION ALLIANCE. Research Report on AI Agent Communication Gateway Technology[M]. Shenzhen: World Fixed Network Innovation Alliance, 2025.

[7] 国家市场监督管理总局, 国家标准化管理委员会. 工业互联网 总体网络架构: GB/T 42021-2022 [S]. 北京: 中国标准出版社, 2022.
STATE ADMINISTRATION FOR MARKET REGULATION, STANDARDIZATION ADMINISTRATION OF THE PEOPLE'S REPUBLIC OF CHINA. Industrial internet—Overall network architecture: GB/T 42021-2022 [S]. Beijing: Standards Press of China, 2022.

[8] 田锐, 徐联智, 方佩, 等. 企业网络IPv6升级改造方案研究[J]. 邮电设计技术, 2022(12): 87-92.
TIAN R, XU L Z, FANG P, et al. Research on IPv6 upgrade and transformation plan for enterprise networks[J]. Designing Techniques of Posts and Telecommunications, 2022(12): 87-92.

[9] 工业互联网产业联盟. 工业互联网网络连接白皮书 [M]. 北京: 工业互联网产业联盟, 2021.
ALLIANCE OF INDUSTRIAL INTERNET. White Paper on Industrial Internet Network Connectivity [M]. Beijing: Alliance of Industrial Internet, 2021.

[10] 中华人民共和国工业和信息化部. 工业互联网 园区网络 总体技术要求: YD/T 6201-2024[S]. 北京: 人民邮电出版社, 2024.
MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY OF THE PEOPLE'S REPUBLIC OF CHINA. Industrial internet—Campus network—Overall technical requirements: YD/T 6201-2024[S]. Beijing: Posts & Telecom Press, 2024.

[11] WANG J H, WANG Y, XU M, et al. Separating identifier from locator with extended DNS[C]//Proceedings of 2012 IEEE In-

ternational Conference on Communications (ICC). Piscataway: IEEE Press, 2012: 2747-2751.

[12] CHEEKIRALLA S, ENGELS D W. An IPv6-based identification scheme[C]//Proceedings of 2006 IEEE International Conference on Communications. Piscataway: IEEE Press, 2006: 281-286.

[13] XIONG R, REN W, HAO X, et al. BDIM: a blockchain-based decentralized identity management scheme for large scale Internet of Things[J]. IEEE Internet of Things Journal, 2023, 10 (24): 22581-22590.

[14] PERERA C, ZASLAVSKY A, CHRISTEN P, et al. Context aware computing for the Internet of Things: a survey[J]. IEEE Communications Surveys & Tutorials, 2014, 16(1): 414-454.

[15] YU H, SHEN Z, LEUNG C. From Internet of Things to Internet of Agents[C]//Proceedings of 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing. Piscataway: IEEE Press, 2013: 1054-1057.

[16] ITU-T. Framework of software-defined networking[M]. Geneva: International Telecommunication Union, 2014.

[17] 丁俐夫，颜钢锋. 多智能体系统安全性问题及防御机制综述[J]. 智能系统学报，2020，15(3): 425-434.
DING L F, YAN G F. Survey on security issues and defense mechanisms in multi-agent systems[J]. Journal of Intelligent Systems, 2020, 15(3): 425-434.

[18] 曲升宇，李柘. 基于 AI STR 框架的工业人工智能体安全治理路径研究[J]. 智能感知工程，2025，2(3): 27-34.
QU S Y, LI Z. Research on security governance path for industrial AI agents based on AI STR framework[J]. Journal of Intelligent Sensing and Engineering, 2025, 2(3): 27-34.

[作者简介]

韩政鑫（1994-），女，硕士，中国联合网络通信有限公司研究院工程师，主要研究方向为下一代互联网、确定性网络、工业互联网等新技术和应用。

韩梦瑶（1995- ），男，博士，中国联合网络通信有限公司研究院工程师，主要研究方向为下一代互联网架构演进与关键技术。

庞冉（1989- ）,男，硕士，中国联合网络通信有限公司研究院正高级工程师，主要研究方向为数据通信、算网一体、下一代互联网等前沿技术。

何涛（1982-），男，硕士，中国联合网络通信有限公司研究院高级工程师，主要研究方向为数据通信、算网融合、智能体互联网等。；

曹畅（1984 -），男，博士，中国联合网络通信有限公司研究院正高级工程师，主要研究方向为数据通信、算力网络、下一代互联网架构与核心技术。；

唐雄燕（1967-），男，博士，中国联合网络通信有限公司研究院副院长、正高级工程师，主要研究方向为光纤传输、宽带通信、算力网络、下一代互联网前沿技术。