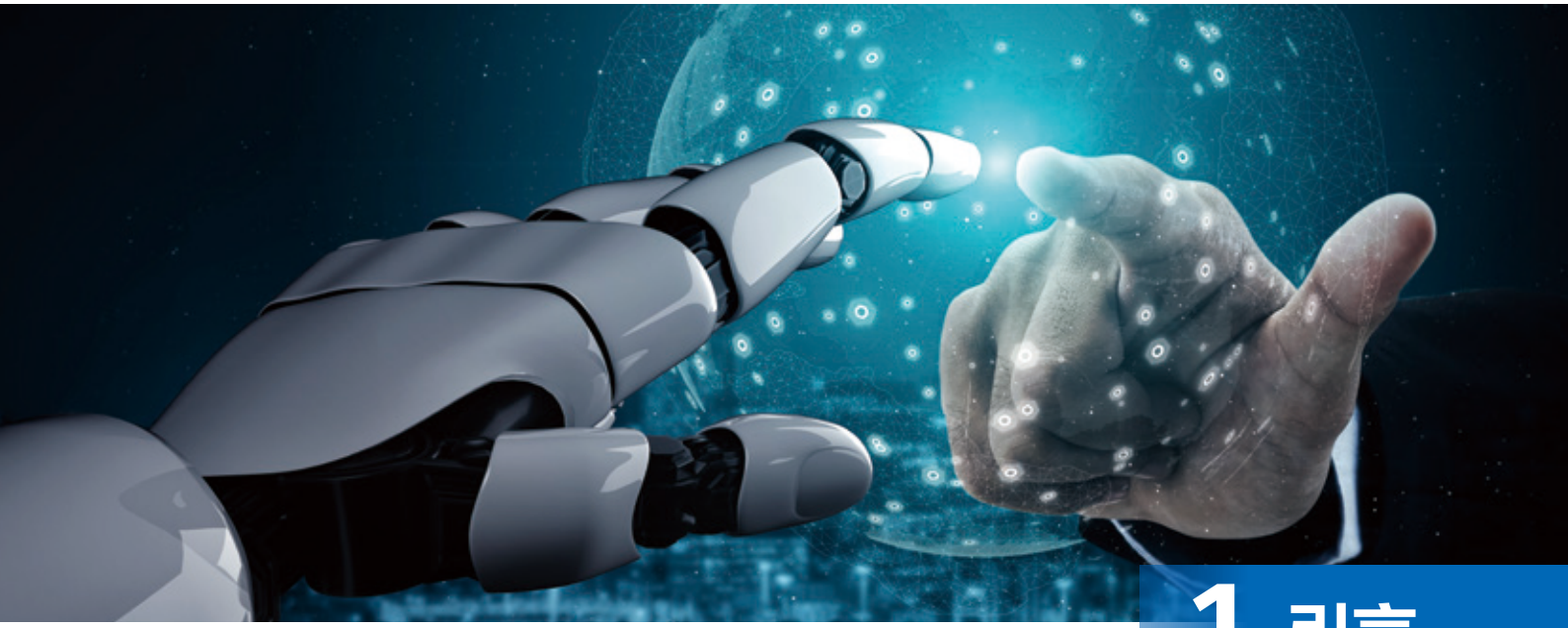
面向智能互联的

网络技术与实践报告V2.0

目录



1 引言

当前，人工智能产业正从大模型能力迭代步入智能体规模化落地与协同互联的关键时期。据产业测算，2026 年全球活跃服务智能体规模将突破千万级，终端智能体在消费电子与工业终端的渗透率达 35%，具身智能体在工业制造、家庭康养等场景的落地量年增速超 120%，三类智能体能力互补、场景协同，共同构筑智能体应用生态的核心形态。然而，单体智能体的能力边界与资源禀赋存在天然局限，跨主体、跨域、跨模态的协同需求持续攀升，推动智能体从 “单体智能” 向 “群体互联” 加速演进，面向智能互联的网络成为人工智能与下一代网络深度融合的核心发展方向。

智能互联正深刻重塑全球网络流量模式与通信特征。区别于传统人机交互下以人为发起端的请求式流量，智能体间的自动化协同催生海量机器到机器的高频、长会话通信，预计未来五年，广域网中智能互联产生的东西向流量占比将从当前不足 10% 提升至 40% 以上，并发连接规模、端到端时延要求与协议复杂度均对现有网络承载架构提出全新挑战，适配智能体通信特征的网络技术体系亟待构建。

与此同时，智能互联的身份体系与治理框架已成为全球标准与产业研究的核心议题。IETF、3GPP、CCSA 等国内外标准化组织已围绕智能体身份标识、分层身份管理、可信互操作协议、合规治理等方向启动十余项专项标准研制，初步形成多维度技术路线，但跨体系互通、权责边界界定、安全监管机制等核心问题仍未形成产业共识，生态碎片化风险逐步显现。

本报告基于2025年《面向智能互联的网络架构与关键技术研究报告》提出的四层总体架构，进一步补充全层级安全与可观测能力，对架构进行深化与优化；依托分层分域设计思路，将智能体通信协作场景精细划分为智能互联局域网、智能互联广域网两类。为破除异构多生态智能体的互联互通壁垒，建设性倡议尽快构建智能体身份管理与注册管理体系，并通过 “管理中心 + 智能体网关” 的分布式一体化架构，实现

智能体入网的可信性、可观测性、安全性与高效性。身份管理体系层面，提出「中心拓展 + 分布式执行」的新型管控分离思路。针对广域网域与行业网域，重点覆盖智能体可信入网的身份管理与接入认证需求。技术路线上支持多种标识技术作为可选方案，整体认证体系设计突出实用性与落地可行性。

报告重点分析智能体网关的基础设施核心定位与能力：一是衔接物理网络与智能体网络的核心桥梁，二是可信入网认证的分布式执行节点，三是保障智能体通信安全、服务质量与运行效率的关键载体。

方案验证与实践层面，报告新增并重点阐释智能体广域网络下的家庭智慧康养、金融行业两大典型应用案例、局域网场景案例，展现面向智能互联的网络在真实业务场景中的应用价值与实践成效。最后，报告提出面向未来的生态建设建议与政策框架，为产业界、学术界及监管部门提供清晰的行动指引。

本报告起草单位：

华为技术有限公司
中国信息通信研究院
NIDA全球固定网络创新联盟
ANP开源社区
中国银联股份有限公司
中国移动通信有限公司研究院
中国电信股份有限公司研究院
中国电信股份有限公司广东分公司
中国联合网络通信有限公司研究院
清华大学
北京面壁智能科技有限责任公司
哈尔滨工业大学

本报告主要起草人：

曹畅、常高伟、尘福兴、邓一鸥、高巍、高强周、金剑、雷波、宋健、王道东、徐明伟、于游、张弛、张恒升、张磊、张雨生、周界、朱科义

注：本报告起草单位和主要起草人排名不分先后。

2 面向智能互联的网络演进与挑战

全球智能体产业正加速从单点工具化应用迈向网络化协同新阶段，智能体也从云中心向端侧下沉，随着具身智能体逐步进入规模化落地周期，终端、具身、服务三类智能体形态并行爆发。截至 2026 年，全球企业级智能体部署渗透率已突破 79%，跨厂商、跨地域、跨网络域的多智能体协同成为核心业务场景，催生出跨广域网协同需求。这一趋势既是智能体技术释放产业价值的核心路径，更成为驱动下一代网络基础设施重构的核心引擎，对底层网络架构提出了全维度的能力升级要求。

智能体具备动态入网、跨域、自主交互的核心特性，传统网络正在面临以下多个挑战。在身份体系层面，需建立统一的分层智能体身份框架，替代传统设备身份认证逻辑，实现智能体入网身份互信、权限分级可控，从接入源头筑牢信任根基。在通信协议层面，需适配智能体注册寻址、状态同步、元数据同步的专属通信协议，构建分布式智能体发现与寻址机制，保障跨域网场景下协同链路的高效建立与状态一致性。在流量调度层面，针对智能体协同流量突发性强、东西向交互占比高的特征，实现基于业务优先级的动态流量调度，为关键协同任务提供确定性时延与带宽保障。

与此同时，智能体自主决策、自主交互的属性，对网络合规治理提出了更高要求，必须满足行为安全交互、可观测、可回溯的目标。传统 Overlay 网络仅能解决基础连通性问题，难以支撑原生的安全管控与服务质量保障。因此，物理网络需内生智能体连接能力，内置基于身份的通信隔离、加密卸载与 QoS 调优机制，搭配全链路可观测探针，实现从物理网络到应用层的全流程行为审计与异常拦截，共同构建可信、可管、可控的智能体网络底座。

当前，产业界与学术界已在流量调度技术、互联协议标准、身份标识体系、交互可观测性、行为安全治理五大核心方向取得阶段性突破：流量模型完成从 “人驱动的南北向下载” 到 “机 – 机协同的东西向交

互”的范式迁移；协议生态从单一私有协议，演进为多标准并行、底层多协议承载的发展格局；身份、寻址、安全、可观测等基础能力体系正逐步成型。

但整体来看，现有技术体系仍基于传统互联网架构做修补式演进，对智能体场景的原生适配性不足，在大上行流量承载、多协议互联互通、全域寻址性能、跨域身份互认、全链路安全可信等方面仍面临系统性挑战。智能体产业的规模化落地，已从 “云内单智能体优化” 转向 “多智能体协作以及互联网络底座构建” 的深水区，亟需打造专门的面向智能互联的网络基础设施，为亿级异构智能体提供统一的身份、寻址、调度、安全与可观测能力支撑。

2.1流量范式变革：从“南北”到“东西”的结构性颠覆与网络挑战

智能体网络的崛起，首先在最基础的层面——网络流量，引发了一场结构性的“地壳运动”。传统的互联网流量以“客户端-服务器”（Client-Server）模型为核心，呈现出典型的“南北向”特征，即终端用户访问中心化的云端服务。然而，多智能体协同的本质，彻底颠覆了这一模式。

2.1.1 流量模式的转变：东西向流量将会成为主导

传统互联网以南北向下行流量为主，下行占比长期高于 85%；而智能体场景下，多智能体状态同步、任务协同、具身感知数据上传推动流量结构剧变。邬贺铨院士在2026 年的专题分析文章《智能体全面重构算力、网络与云，集体智能涌现》中的数据显示，智能互联场景中东西向流量占比将提升至 80%，上行流量占比从传统的 10%-15% 增长至 40%-50%，工业产线多智能体协同场景的东西向流量占比已达 65% 以上。具身智能体单设备上行带宽需求可达 200Mbps 以上，包含 4K 视频、点云、力觉等多模态感知流，形成持续的大上行压力。因此，业界已形成普遍共识并观测到明确趋势，智能体间的通信流量（即“东西向”流量）正在超越传统的“南北向”流量，成为网络负载的主体。智能体为了完成一个复杂任务（例如，一个企业的自动化供应链管理），需要调用分布在不同云、边缘节点或终端设备上的其他专业智能体（如订单处理智能体、物流调度智能体、库存分析智能体等）。这种交互是网状的、分布式的。

行业预测数据显示，这一转变的速度惊人。早在2022年，研究就已指出流量方向正从南北向转变为东西向与南北向并存 。而根据对智算中心和大规模智能体应用部署的最新分析，到2026年底，数据中心内部和跨数据中心的“东西向”流量占比预计将达到惊人的80% 。这种转变不仅仅是方向上的变化，更是流量特征的质变：

- 大上行与对称性： 不同于传统以下行为主的模式，智能体既是服务的消费者，也是能力的提供者。终端智能体（如家庭服务机器人、智能汽车）会持续上传大量的传感器数据、环境模型和状态更新，形成“大上行”流量。这使得上下行流量趋于对等 。
- 高频短连接与混合负载： 大模型推理和检索增强生成（RAG）带来了高频次、小数据包的交互请求，导致每秒查询率（QPS）相比传统应用提升了10到100倍 。同时，智能体间的知识库同步、模型更新又会产生突发的大流量。这种“高频小包+偶发大流”的混合模式，对网络的抖动和带宽都提出了极致要求。

- 长会话与状态维持： 多个智能体在执行一个长期任务时，会建立持续的通信会话，以维持任务上下文、共享状态和协同决策 。这要求网络具备维持大量并发长连接的能力，并且对连接中断的容忍度极低。

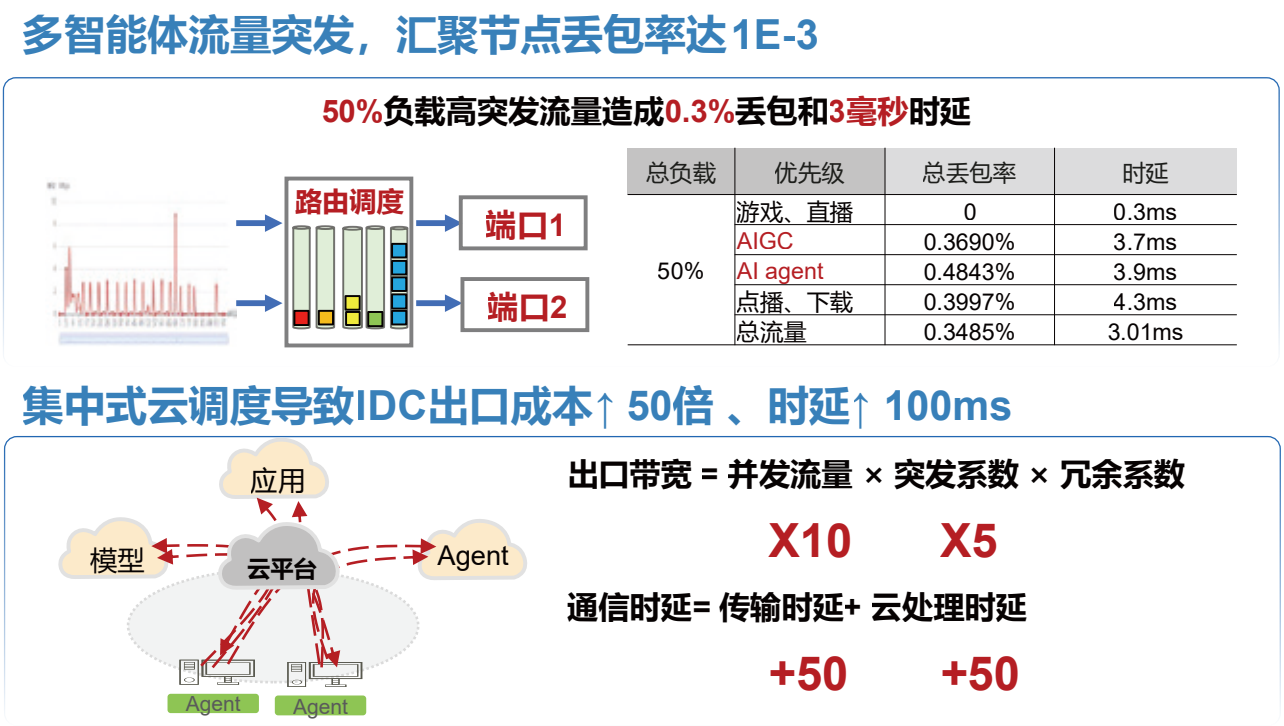


图1 智能体流量流向、流量模型变化对网络架构、调度和路由带来挑战

2.1.2 网络面临的严峻挑战：流量调度

这种全新的流量范式给现有的网络架构带来了两大严峻挑战：

1. 关键节点的拥塞与丢包激增：在智能体协同场景中，一个任务决策可能需要聚合来自成百上千个分布式智能体的信息。这些信息流在网络拓扑中汇聚到某个关键节点或网关（即家庭BNG、云入口等节点）。由于智能体行为的突发性和同步性（例如，对某一热点事件的集体响应），极易在收敛节点处形成流量风暴，导致交换机或路由器的缓冲区瞬间被填满，从而引发大规模丢包。

虽然截至2026年，尚无专门针对“东西向流量占比80%”场景下汇聚节点丢包率的公开、标准化实测基准，但早期在P2P（Peer-to-Peer，）网络和数据中心网络中的研究已经揭示了问题的严重性。例如，在模拟高负载P2P网络的研究中，当网络负载增加时，即使只是从10%增加到20%，流量丢包率也可能出现显著上升。在智能体网络中，流量的脉冲性和同步性远超传统P2P应用。我们可以合理推断，在智能体协同的峰值时刻，未经优化的网络汇聚节点丢包率可能从常规的低于0.1%飙升至5%-10%甚至更高，这将直接导致智能体协同失败、决策错误或任务超时。这要求网络基础设施必须从被动承载转向主动感知和调度，例如通过SRv6、云网虚拟化和流量AI预测等技术，提前疏导和保障确定性路径。

2. 类P2P通信带来的调度挑战：智能体间的网状通信模式，本质上是一种大规模、异构的对等网络（P2P）。这使得传统的、基于中心化控制的流量调度策略捉襟见肘。如何为数以亿计的智能体间交互动态地寻找最佳通信路径，成为一个极其复杂的NP-hard问题。

- 路径发现与选择： 如何在海量智能体中快速、准确地找到目标智能体，并规划一条满足延迟、带宽、成本等多维约束的路径?
- 拥塞控制： 传统的TCP拥塞控制机制主要为南北向长连接设计，难以适应东西向流量的短、快、多变特征。
- 资源分配： 在全局网络资源有限的情况下，如何公平且高效地为不同优先级的智能体任务分配带宽?

为了应对这些挑战，学术界和产业界正积极探索新的调度算法，比如一个备受瞩目的方向是基于强化学习（RL）的智能调度方法，相比传统方法，能在复杂网络环境下显著提高吞吐量、降低延迟，并更快地达到收敛状态 。尽管这些技术在模拟环境中展现出巨大潜力，并在部分CDN和P2P分发场景中得到应用但如何将其扩展到亿万级、跨域、异构的面向智能互联的网络，并保证其决策的实时性和鲁棒性，仍然是一个开放的、极具挑战性的研究课题 。

2.2 协议探索，智能互联的标准化进展

如果说流量模式是智能互联的“物理表现”，那么通信协议就是其沟通的“语法规则”。缺乏统一的协议，智能体之间将如同“巴别塔”中的人们，无法有效协作。截至2026年，智能体通信协议的标准化已从早期的概念探讨进入了实质性的草案制定和产业实践阶段，但距离全球统一仍有一段路要走。

在2024年之前，业界存在多种自研或小范围的智能体交互协议，如早期的A2A（Agent2Agent Protocol）、Agent Network Protocol (ANP) 以及一些企业内部的通信规范（ACP）。这些协议虽然在特定场景下解决了问题，但也形成了新的“技术孤岛”，阻碍了跨平台、跨厂商智能体的广泛互联。因此，全球的标准化组织和产业联盟开始加速行动。其中，互联网工程任务组（IETF）作为互联网协议的权威制定者，已成为推动智能体通信协议全球标准化的核心力量 。IETF成立了专门的工作组和兴趣小组，旨在为广域互联、跨域互通的智能体网络制定一套开放、安全、可扩展的协议栈 。在近期的IETF会议（如IETF 125）上，关于AI协议的讨论和草案提交变得异常活跃 。与此同时，中国在国家层面也取得了显著进展，全国信标委人工智能分委会已牵头立项了智能互联的系列国家标准，涵盖总体架构、身份、交互等多个方面，预计部分标准将在不久后完成报批。

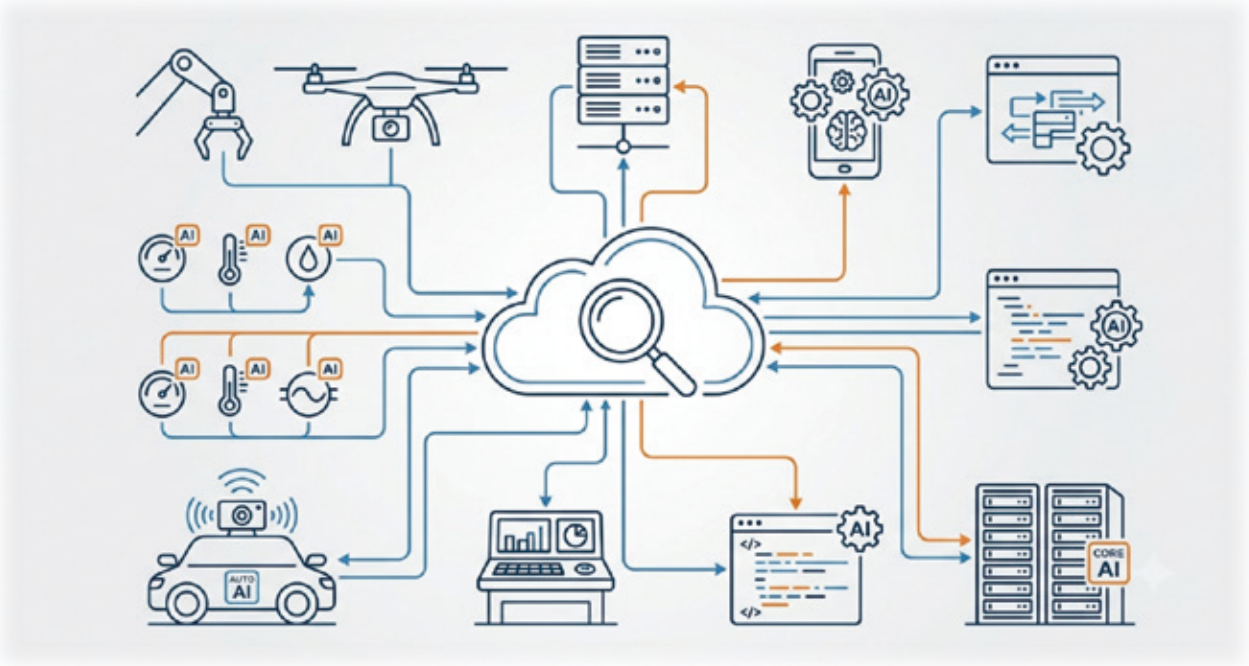


图2 多智能体异构、跨域协同与通信，对智能体网络的多协议承载及适配的需求

IETF新兴协议草案，在众多提案中，一套层次化的协议栈概念逐渐清晰，旨在解决智能体生命周期中的关键通信问题。其中，以下三个处于草案阶段的协议尤为引人注目，它们共同勾勒出未来智能互联通信的骨架：

1. 主流协议生态持续演进：当前已形成 MCP、A2A、ACP、ANP 四大主流协议体系，分别覆盖工具调用、点对点协作、企业内网群体协同、全域开放互联四大场景。其中 MCP 已成为智能体工具调用事实标准，官方服务器数量突破 15000个；A2A 协议定义了能力卡片、任务外包等交互原语，是跨平台智能体协同的主流方案；ACP 由 IBM 主导，适配企业级多模态交互场景；ANP面向智能体在互联网上的跨域连接与协作。

2. IETF 新型协议草案加速推进：IETF 已成立 CATALIST BoF 工作组，系统性推进智能互联底层标准，在 IETF 125 会议上形成 16 项专题研讨成果，明确了注册发现、元数据同步、传输承载三大核心协议方向，对应形成智能体注册发现协议、智能体元数据同步协议、智能体消息传输协议等标准草案雏形。

a.智能体注册与发现协议：旨在解决智能体“如何被找到”以及“它能做什么”的问题。它定义了一套标准机制，允许智能体向一个或多个注册中心（Registry）发布自己的身份、能力（如提供的服务、可调用的工具）、网络地址、公钥以及其他元数据 。其他智能体则可以通过查询这些注册中心，来发现满足其任务需求的协作者。该部分设计强调了服务目录和注册中心的分层结构，以应对全球规模的智能体发现需求 。

b.智能体元数据同步协议：是面向智能互联的网络控制面的核心网关间协议，聚焦跨管理域的元数据同步底座能力。当智能体通过元数据同步 完成本地注册后，其身份、能力、可达性、安全属性等核心元数据

会通过层级化的智能体网关，实现跨域同步与全局分发。元数据同步协议旨在为多级网关提供高效、一致、无环的元数据同步机制，支撑各网关生成全局统一的智能体转发表，保障跨域异构智能体的全局可达与能力寻址，为上层注册发现、消息路由、安全管控提供标准化的元数据底座。当前元数据同步协议已形成正式的 IETF 标准草案，明确了分层网关同步架构、Agent Record 元数据格式与推拉混合同步模型，完成了协议的基础框架定义。

c.智能体消息传输协议：致力于解决智能体之间“如何可靠通信”的底层传输问题。它并非要取代TCP或QUIC，而是作为一个更高层次的、面向消息的传输协议，提供包括持久化消息、事务性保证、端到端加密、优先级队列、以及针对智能体交互特有的“意图（Intent）”传递等高级功能。

综合来看，智能互联协议的标准化正在从“群雄逐鹿”走向“合纵连横”。在IETF众多新兴协议草案为构建一个开放、分层的智能体通信体系结构指明了方向。然而，这套体系对网络基础设施提出了多协议承载与互联互通的根本要求。未来的面向智能互联的网络必须能够高效地处理和转发多种新兴协议报文，并提供协议间的翻译或网关能力，以兼容海量的异构智能体生态。

2.3 数字身份，智能体协同的信任基石与跨域互认挑战

如果说协议是沟通的语言，那么身份就是信任的起点。在一个由自主智能体构成的社会中，一个清晰、可验证、可追溯的身份体系，是进行一切可信交互、授权和追责的基础。

2.3.1 产业痛点与标准化先行

传统身份与访问控制机制失效，传统安全体系的根基是为“人”设计的，其基本假设与智能体的行为模式完全相悖。

- 静态与长周期的身份模型：传统的IAM系统，无论是基于用户名/密码，还是基于X.509证书，都假设身份是相对静态且长周期的。一个员工的身份可能数年不变。而智能体，特别是用于执行特定任务的微智能体（Micro-agent），其生命周期可能只有几秒钟。为每个短暂的智能体手动配置和管理静态凭证，在操作上是不可行的，并且会留下大量的“僵尸凭证”，构成巨大的安全风险。
- 管控模式从静态授权向动态零信任演进。传统基于角色的访问控制（RBAC）依托固定组织关系与预设权限，适用于稳态的人员与系统；智能体跨域协作具有临时性、动态性特征，无固定组织关系依托，推动管控模式向基于事务、基于意图的动态授权升级。零信任架构向智能体场景延伸，形成 “永不信任、始终验证” 的管控原则，对每一次交互、每一次工具调用都进行身份与权限校验。
- 身份管理从单域管理向全域互认演进。当前智能体身份体系分属不同平台与管理域，各自独立；随着跨域协作普及，身份互认需求持续增长，业界开始探索联邦式身份治理体系，通过统一的身份标准与信任锚，实现跨域身份的可信核验与权限互认，避免重复认证与重复授权。

图3 传统认证面向人设计，智能体入网身份带来新的认证与攻击挑战

这种不匹配导致了一系列新型安全风险：

- 身份仿冒与女巫攻击（Sybil Attack）：恶意智能体可以轻易伪装成合法智能体，进行欺诈、窃取数据或发起攻击，或者在去中心化共识系统中污染投票结果。
- 权责不清： 当多个智能体协同完成的任务出现问题时，无法准确追溯到是哪个智能体的行为导致的。
- 跨域协同困难： 两个来自不同生态的智能体无法相互验证对方的身份，建立信任关系，从而无法进行有意义的协作。
- 凭证泄露与横向移动：智能体在调用工具或API时，通常需要处理和存储API密钥、数据库密码等敏感凭证。一旦智能体被攻破，这些凭证就会泄露，攻击者可以利用它们在网络内部进行横向移动，扩大攻击范围。

为了解决这些问题，中国在国家标准层面走在了前列。“人工智能 智能互联”系列国家标准明确将身份管理作为核心组成部分，正在制定包括智能体身份编码规则、身份管理机制、以及基于身份的权限控制等规范 。这些标准旨在通过为每个智能体分配一个唯一的、符合国家规范的“数字身份证”，从源头上解决身份不统一的问题，为构建跨平台的智能体信任体系奠定基础。

2.3.2 学术与产业的技术探索：中心化、分布式并行

与标准化并行，学术界和产业界正在探索实现智能体身份系统的具体技术路径，并逐渐形成从中心化向去中心化演进的趋势。

- 中心化身份管理： 当前企业以及云内服务，正在构建中心化的智能体安全互通平台。这些平台提供智能体注册认证、全生命周期身份管理、以及基于身份的细粒度权限鉴权等能力 。其优势在于易于管理、快速部署，并能与现有的网络管理和安全体系紧密结合。例如，通过一个中心化的身份网关，可以对所有入网的智能体进行强制认证和权限检查。
- 分布式身份（DID）探索： 然而，中心化的身份系统也存在单点故障、隐私泄露以及被单一实体控制的风险。因此，学术界和前沿技术社区更倾向于探索基于去中心化标识符（Decentralized Identifiers, DID）和可验证凭证（Verifiable Credentials, VC）的方案 。
  - DID 赋予智能体自主控制、不依赖中心化机构的全局唯一身份，为保障全局身份的统一性与不可抵赖性，研究呈现利用区块链技术的趋势。
  - VC 则允许一个智能体（如一个行业协会认证的智能体）向另一个智能体出示一个由权威第三方签发的、可被密码学验证的“能力证书”或“资质证明”（例如，“我是一个通过认证的医疗咨询智能体”）。

基于DID+区块链和VC的体系，有望从根本上解决跨域信任问题。两个素不相识的智能体，无需预先共享密钥或信任同一个中心平台，只需通过交换和验证彼此的VC，就能建立起临时的、基于密码学保证的信任关系 。

2.3.3 终极挑战：跨域互通与互认的“信任鸿沟”

尽管技术路径日益清晰，但实现真正意义上的全球智能体身份跨域互通互认，仍面临巨大的“信任鸿沟”：

1.传统身份机制无法适配智能体动态特性：面向人的 IAM 与 NAC 体系，以账号、终端为管理对象，生命周期长、状态稳定；而智能体实例可动态生成与销毁，临时子智能体生命周期可短至 30 秒，身份的申请、认证、注销需全自动化完成，传统人工审批、静态配置的模式完全失效。同时智能体数量呈亿级规模，远超人员与终端数量级，对身份系统的并发处理能力提出量级式挑战。

2.新型攻击风险凸显，安全管控边界模糊：智能体开放互联后面临提示注入、女巫攻击、决策影响等新型安全风险，攻击者可通过伪造虚假智能体身份、注入恶意指令等方式干扰协同过程。传统基于边界的防护体系无法识别智能体层面的恶意行为，基于角色的权限控制难以适配无固定组织关系的跨域智能体交互，易出现权限越界与级联放大风险。

3.信任根的建立： 去中心化信任并非没有信任，而是将信任从中心化平台转移到了“信任根”（Trust Anchor），即VC的签发者。如何建立和管理一个全球公认的、分层次的信任根体系？谁来扮演这些角色？如何确保签发者的权威性和公正性？

4.份管理与合规框架： 智能体的身份不仅仅是技术问题，更是合规与治理问题。智能体的法律主体地位如何界定？当一个拥有合法身份的智能体产生侵权行为时，其所有者、开发者和使用者应如何承担责任？这些问题都需要跨学科的深入研究和顶层设计。

因此，面向智能互联的网络基础设施必须内建对多种身份体系的兼容和转换能力。网络本身需要成为一个“信任中介层”，能够解析来自不同身份系统的标识，并根据预设的策略和信任链，在不同信任域之间进

行身份映射和权限转译，从而弥合信任鸿沟，使大规模跨域协同成为可能。

2.4 智能体行为观测的需求与挑战

2.4.1 面向智能互联的网络可观测性的核心挑战

传统集中式观测模式依赖网络节点采集数据后回传中心统一分析，仅适用于小范围、同架构的网络运维场景。随着智能体呈现跨多层、跨域、跨生态的运行特征，纯中心化集约观测模式加速失效，行业整体陷入“行为不可控、链路不可测、责任不可追”的核心困境，具体挑战体现在四个维度：

1. 智能体行为黑盒化，合规合理性监测难度大

智能体具备高度自主决策能力，行为路径与推理逻辑动态可变。传统观测仅能采集 IP 层流量等底层网络数据，无法穿透智能体的决策与执行逻辑，既不能识别智能体身份、交互意图与行为合规性，也难以对“影子智能体” 非法接入、越权交互、目标偏离等违规行为实现实时精准管控。同时智能体决策的非确定性导致异常行为判定缺乏明确基准，异常检测的误报率与漏报率居高不下，行为监管存在大面积盲区。

2. 跨域链路多跳多层，质差问题根因定位效率低

智能体跨域交互需经过多跳网络节点、多层协议转换，链路路径长、转发关系复杂，高时延、丢包、拥塞等通信质差问题频发。传统分段式中心化观测仅能掌握单域局部数据，无法串联跨生态、跨运营主体的多段链路，难以形成完整的端到端观测视图；出现通信质差或业务故障时无法快速界定故障域，平均排障时长超过 24 小时，远高于单域场景的分钟级排障效率。此外全量数据回传中心分析的模式处理效率低，难以适配动态变化的通信路径，质差处置成本高、响应慢。

3. 跨生态数据相互割裂，责任溯源与定界难度大

智能体交互横跨多个独立生态平台，各方日志标准不统一、数据相互割裂，缺乏统一的全链路交互溯源机制。当出现服务异常、数据泄露、业务损失等问题时，无法清晰界定不同生态主体、不同网络节点的责任边界，纠纷处置与治理效率低下，中心化观测体系无法打通异构生态的数据壁垒实现统一追责。

4. 统一观测标准缺失，体系化建设滞后且成本失衡

当前行业尚未形成统一的智能体可观测性指标体系、数据格式与接口规范，不同厂商的观测工具数据不互通、指标不可比，无法形成全网统一的观测能力。同时，全量存储智能体交互与推理数据会带来极高的存储与算力成本，行业尚未形成在保障可追溯性的同时控制成本的成熟技术方案，制约了可观测体系的规模化落地。

2.4.2 面向智能互联的网络可观测能力的核心需求与发展方向

针对中心化观测模式的失效与上述核心挑战，面向智能互联的网络需构建分层覆盖、多维度联动、分布式智能感知的一体化可观测体系，推动观测能力从基础设施层向行为层延伸、从单域闭环向跨域协同演进，最终实现 “行为可管、链路可测、责任可追” 的治理目标。

1. 分层级核心能力需求，围绕智能互联的全链路流程，需在应用层、注册 / 发现层、网络层全域部署观测点，形成多层协同的观测能力：

- 应用层：端到端行为与质差观测，支撑全链路交互溯源，覆盖智能体 “消息传输 – 推理决策 – 工具调用 – 跨体协同 – 结果输出” 全业务流程，采集调用请求、响应结果、执行路径等应用层数据，完整还原智能体行为路径；同步监测应用级时延、调用失败率等质差指标，支撑异常行为识别、合规性校验与交互问题根因追溯，从业务层面破解 “行为不可控” 难题。
- 注册 / 发现层：全量交互日志留存，构建全局关系画像，完整记录智能体注册、发现、服务调用的全量日志，基于日志开展 TopN 调用统计、多智能体交互关系画像构建，清晰呈现智能体间的依赖关系与调用拓扑，为全局流量调度、风险预判、生态治理提供数据支撑。
- 网络层：分布式智能观测分析，实现流量与质差精准感知，突破纯中心化分析模式，赋予网络节点针对智能体的本地智能观测能力，就地识别交互异常、流量异常模式；同步开展跨域多跳链路的时延、丢包、带宽等网络质差指标监测，通过网络层数据与上层业务数据的联动分析，实现质差问题的快速根因定位，破解 “链路不可测” 难题。

2. 整体演进方向

- 观测边界延伸：从基础设施监测向行为合规审计升级，观测对象从链路时延、丢包、带宽等网络性能指标，延伸至智能体全生命周期行为，实现从性能监测向行为追溯、合规审计的能力升级，精准回应 “交互是否合规、失败根因是什么、责任如何界定” 等核心治理问题。
- 架构模式演进：从单域闭环向跨域联邦协同发展，打破平台内、域内闭环的观测局限，探索联邦式可观测架构，在保护各方数据隐私的前提下，实现跨域交互链路的端到端追溯与故障定界，适配智能体广域互联的发展趋势。
- 指标体系统一：从通用零散向分层标准化迭代，基于智能互联的分层架构，构建网络层、传输层、交互层、业务层的分层观测指标体系，统一数据格式与接口规范，为全网协同观测提供标准依据；同时探索轻量化存储与分析方案，平衡可追溯性与部署成本。

可观测性是面向智能互联的网络可信运行的基础。只有构建分层、语义丰富的监测体系，破解跨域上下文传播与数据协同难题，才能揭开智能体行为的 “黑箱”，建成可解释、可审计、可管控的面向智能互联的网络，为产业规模化落地提供可信保障。

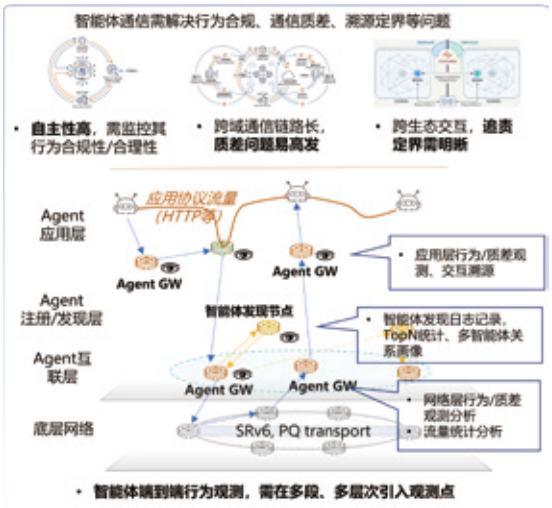


图4 智能体跨广域交互的可观测性挑战

2.5 智能互联的内生安全需求与挑战

智能体的引入，不仅继承了传统软件的所有安全风险，更开辟了全新的、更为复杂的攻击面。这些攻击面不再局限于网络边界或应用代码，而是渗透到了模型的逻辑、工具的交互和数据的记忆中。传统的网络安全手段，如防火墙、WAF（Web应用防火墙）和杀毒软件，对于这些新型的、基于语义和逻辑的攻击几乎无能为力。构建面向智能互联的网络的安全防护体系，必须采用一种全新的、贯穿全链路的深度防御（Defense-in-Depth）思想。

2.5.1 智能体安全防护变化与需求

智能互联将安全边界从传统的网络边界、系统边界，延伸至模型、智能体、工具、数据全维度，推动安全防护体系从单点被动防御向全链路内生安全演进，呈现三大变化与趋势：

1. 防护范围从网络层向模型 – 智能体 – 工具 – 数据全链路延伸。传统网络安全聚焦传输层与网络层的攻击防护；智能体场景下，攻击面扩展至模型层、工具层、数据层三大维度，安全防护随之向全链路覆盖，形成 “模型安全 – 智能体安全 – 工具安全 – 数据安全 – 传输安全” 的多层防护体系。

2. 防护重心从内容安全向行为安全转移。传统 AI 安全以内容合规为核心，聚焦输出内容的有害性治理；智能体具备自主行动能力，行为风险的危害性远高于内容风险，因此防护重心向行为安全升级，通过行为围栏、动态审计、意图校验等技术，界定智能体自主决策的安全边界，防范越权操作与恶意行为。

3. 防护模式从静态边界防御向动态内生安全演进。传统边界防御依赖固定的安全网关与策略配置，无法适配智能体动态拓扑与开放互联的特征；安全防护正在向内生安全方向发展，将安全能力内嵌至互联网络的各层级，实现安全能力与网络架构的原生融合，支撑动态、全场景的安全防护。

2.5.2 面向智能互联的网络安全挑战

智能互联带来的全新攻击面，使传统安全体系面临防护失效的风险，核心挑战集中在三个维度：

1. 新型攻击面持续扩大，传统安全手段覆盖不足。智能体引入模型藏毒、提示词注入、API 越权访问、数据泄露、记忆投毒等新型攻击方式，攻击从网络层上升至逻辑层与语义层，传统防火墙、入侵检测等网络安全手段无法识别与拦截。据中国信通院 2026 年测试数据，智能体行为有害率普遍高于 14%，最高可达 36%，远高于内容有害率，行为层面的安全防护能力严重不足。

2. 跨域交互安全缺乏原生支撑。跨域智能体交互时，缺乏统一的安全入网校验机制，难以快速确认对方智能体的安全资质与可信等级；交互消息的端到端加密、防篡改、抗抵赖能力缺失，易出现指令篡改、数据窃听等风险；同时跨域安全事件的溯源与定责机制空白，出现安全事件后难以追溯攻击来源与界定责任。

3. 全链路安全协同能力不足。当前模型安全、智能体及交互安全、工具安全、数据安全、网络安全分属不同技术领域与管理部门，各防护体系独立运行，缺乏协同联动机制。攻击发生时，无法实现从网络层到应用层的联动处置，攻击响应时延长、处置效率低，难以应对智能体场景下快速扩散的安全风险。

3 智能体网络总体架构与协议

3.1 架构及协议设计原则

面向智能互联的网络是面向自治智能体跨域协同交互的新型网络架构，区别于传统面向人机交互的互联网体系，其架构设计围绕智能体自主协作、动态组网、任务化交互的核心特征，提出协作解耦、不中断、自主性、开放互联四大设计原则，加速智能体异构互通、跨域协同在架构、协议的研究与收敛。

1.协作解耦原则

协同解耦原则：智能体应用开发的时候不假设它需要和谁互联和协作，智能体不因为互联协作改变其内部业务逻辑、运行机制与部署，智能体不感知其他智能体，它只向网络提交或接受任务，接受或回复交付件，而不关心整体任务有哪些智能体参与。网络承担任务语义寻址、交互调度、消息投递的中间枢纽能力，彻底解耦智能体的局部业务实现与全局协同关系，确保智能体不会因外部互联协作需求改造自身业务逻辑与运行状态。

2.不中断原则

不中断原则：在多智能体协同任务场景中，任意参与智能体在任务生命周期内可自由上线加入、离线退出、动态迁移或异常重启，且单一智能体的状态变动不会引发全局任务中断、回滚或重启，也不会改变其余在线智能体的运行状态与任务进度。网络需具备任务上下文缓存、断点接续能力，将个体智能体的异常故障与全局协同任务解耦，保障多智能体协作系统的高稳定性、高弹性与高可用性，适配智能体动态、无序、长时间的协同工作模式。

3.自主性原则

自主性原则：智能体间相互发现、通信、协作无需人工参与、预设配置或指令干预。网络支持异构智能体

基于自身任务需求与能力特征，自主完成网络接入、邻居发现、身份可信校验、通信链路建立、协作关系匹配、任务分工协商与动态交互迭代，可独立完成完整的协同业务闭环。摆脱传统网络依赖人工配置、主动触发、预设交互逻辑的运行模式，实现智能体之间的**自发现、自连通、自协商、自协作**。

4.开放互联原则

开放互联原则：智能体通信需要打破传统软件交互依赖预设接口、定制协议、事前适配的互通壁垒，构建全域开放的智能体协同体系。任意异构、跨域智能体，无需提前约定专属通信协议、固定API接口与交互规范，即可依托面向智能互联的网络的统一交互范式与标准化网关，实现跨厂商、跨平台、跨域、跨架构的通信交互与任务协作。网络需要支持通信适配、语义解析、协议转换能力屏蔽底层个体差异，实现无预设、强开放、全兼容的智能体全域互联互通。

3.2 "4+2"架构详解

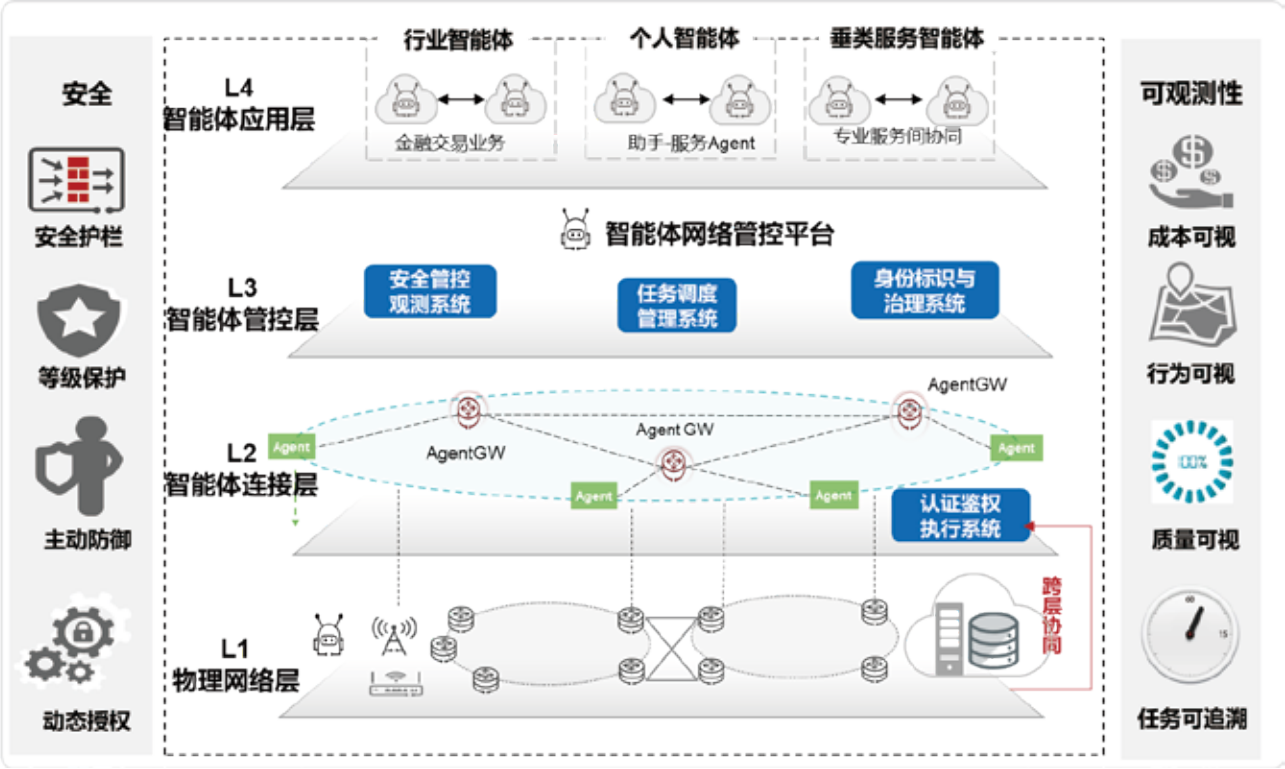


图5 面向智能互联的网络的4+2架构全景图

层级	名称	核心功能
L1	物理网络层	物理网络层为智能体通信提供连接底座，以IP网络基础设施为核心，整合云数据中心、边缘节点、无线网络设施，承载全域计算、存储物理资源，实现云边端跨域智能体泛在互联与资源全域可达。
L2	智能体网络连接层	智能体网络连接层在物理网络之上，基于智能体网关构筑一张逻辑连接网络。为智能体通信提供语义路由、任务调度、上下文缓存/分发、接入控制执行等能力。

层级	名称	核心功能
L3	智能体网络管控层	通过构建分域智能体注册中心，负责智能体身份、技能与能力的注册、认证授权、能力评估、状态更新、吊销等全生命周期管理。
L4	智能体应用业务层	提供智能体通信标准化接口，负责智能体任务管理、能力发现、状态更新、能力协商等功能。
Z1	智能体网络安全	覆盖全部四层，提供端到端的安全保障，包括身份安全、通信安全、数据安全、行为审计等。
Z2	智能体网络可观测	覆盖全部四层，提供网络可视、流量监测、性能追溯、异常检测、日志审计等能力。

3.2.1 智能体物理网络层

物理网络层是面向智能互联的网络的底层承载底座，承接云数据中心、边缘计算节点、无线网络等全域基础设施资源，为智能体自主协同、任务化交互提供基础网络连通、资源调度与数据传输能力。相较于传统以人为核心的互联网架构，智能体与智能体的自治交互范式，彻底颠覆了传统网络的连接模式、流量模型与服务架构，催生物理网络层的全方位重构。传统物理网络适配人机交互的数据共享需求，而面向智能互联的网络以任务执行为核心，流量特征、连接形态与调度逻辑的根本性变化，倒逼物理网络层重塑核心功能，适配智能体高并发、高突发、大上行、高东西向流量的传输需求。

面向智能互联的网络首先实现了网络连接模式的根本性变革，彻底扭转了传统互联网的流量传输逻辑与网络架构适配逻辑。传统互联网以人类浏览、检索、下载的数据共享需求为核心，交互模式以终端主动拉取数据为主，下行流量占据绝对主导地位，网络架构采用自上而下的收敛式设计，适配“中心下发、终端接收”的单向流量特征。而面向智能互联的网络的核心是多智能体自主任务执行与协同交互，交互逻辑由被动拉取数据转变为主动推送任务、交付结果、同步状态，形成以**上行推送为核心**的传输模式。这种模式变革带来了流量结构的颠覆性变化，智能体场景下终端上行流量呈十倍级增长，网络上下行流量比例由传统的1:10趋近于1:1，彻底打破了传统网络非对称的流量格局。

传统收敛式网络架构与智能体全新流量模式存在天然适配冲突，引发一系列网络性能问题。传统分层收敛架构面对海量智能体同时上行推送数据的场景，极易形成“多打一”的流量突发拥塞，经实测与理论推导，该场景下网络丢包率将升至10^{-3}量级，同时队列拥塞会额外引入5ms左右的排队时延，直接影响智能体任务执行的实时性与稳定性。在 无线接入场景中，大上行、高并发的智能体流量会大幅加剧信道竞争冲突，使WIFI网络冲突概率提升8倍，直接导致无线网络并发性能下降30%，无法满足多智能体同时在线协同的基础接入需求。由此可见，传统面向下行优化、收敛式部署的物理网络架构，已完全不适配智

能体任务化、主动推送式的交互场景。

除连接模式外，智能体机机自主交互的特性，彻底重构了网络流量模型，对物理网络传输质量提出严苛约束。传统互联网为人机交互，流量具备平缓、可控、低突发的特征，流量峰均比低。而面向智能互联的网络为无人自治的机机交互模式，流量呈现出**超高峰均比、超高小包占比、高并发、强突发、短生命周期**的典型特征。在多智能体协同任务中，心跳同步、指令协商、状态上报、结果交付等交互行为，产生大量高频小包流量，全网小包流量占比超80%，同时任务的瞬时启动、批量调度会引发流量突发，使智能体流量峰均比达到传统人机流量的10倍。这种极端流量特征，对物理网络的时延稳定性、带宽动态调度能力、突发拥塞控制能力提出极高挑战，传统静态带宽分配、慢速路由调度的物理网络机制，无法适配智能体流量的动态变化，易出现时延抖动、瞬时丢包、并发阻塞等问题。

在网络服务架构层面，智能体协同彻底打破了传统互联网中心化C/S服务模式，重塑了全网流量流向分布，对云中心调度架构形成颠覆性冲击。传统网络以云数据中心为核心，采用客户端-服务器单点交互模式，流量南北向收敛至云中心处理，东西向跨终端、跨节点流量占比极低。而智能体自主、对等的协同特性，催生了多点Mesh组网、点到多点联动的新型连接模式，大量智能体之间的本地协同、跨边缘节点交互无需经过云中心，使网络东西向流量占比大幅提升至40%。传统以云为绝对核心的调度架构，所有跨域交互、资源调度、任务协商均需上云处理，大量东西向流量跨长链路往返云端，会引入百毫秒级额外时延，同时大幅增加云中心出口带宽压力，使云出口流量负载提升50倍，造成云端算力、带宽资源浪费与全网调度低效。

面对连接模式、流量模型、服务架构的三重变革与核心挑战，面向智能互联的网络对传统物理网络进行全方位重构，重新定义物理网络层的核心功能与运行机制，形成适配A2A自治协同的新型物理网络底座。

接入网络：重塑无线网络调度机制，优化WIFI信道竞争、上行资源分配策略，破解大并发、大上行流量引发的信道冲突问题，降低无线性能损耗，恢复多智能体无线并发协同能力。

承载网络：革新网络路由调度机制，针对智能体流量高突发、高并发、小包密集、生命周期短的特征，优化动态路由与拥塞控制算法，提升网络对瞬时流量峰值的适配能力，降低小包转发时延与排队损耗，保障智能体高频、短时、突发式交互的传输稳定性。

网络架构：重构网络流量承载架构，优化传统单向收敛、下行优先的设计逻辑，构建上下行对等的扁平化承载架构，重点强化大上行流量承载能力，解决智能体主动推送场景下的拥塞丢包、时延超标问题，适配1:1的上下行流量新格局。

流量调度：重构全网调度架构，打破单一云中心调度模式，推动调度能力向边缘计算节点延伸，构建“云-边-端”分层调度体系。针对海量东西向智能体流量，实现边缘本地闭环调度，无需云端中转，大幅降低跨域传输时延与云端出口带宽压力，实现全网资源高效利用。

综上，面向智能互联的网络物理网络层的核心作用，是通过架构、路由、无线、调度机制的全方位重构，适配智能体任务化、自治化、对等化的交互特征，解决传统网络大上行适配不足、突发流量承载薄弱、东西向调度低效、无线并发性能差等核心痛点。通过重塑物理层基础能力，为上层智能体自主发现、动态协同、不间断任务执行提供低时延、低丢包、高并发、高弹性的全域网络承载支撑，是实现面向智能互联的网络四大核心设计原则、保障全域智能体高效协同的底层硬件与网络基础保障。

3.2.2 智能体网络连接层

智能体连接层是面向智能互联的网络承上启下的核心中间层，部署于物理网络底座之上、智能体网络管控层之下，是适配智能体开放互联、长周期协同、动态组网的关键公共基础设施。相较于传统互联网仅承担数据透明传输的基础功能，智能体网络连接层依托Overlay架构重构应用通信逻辑，适配智能体时代开放化、异步化、动态化、超大规模化的新型通信需求。从Web互联网、移动互联网到面向智能互联的网络，应用架构与通信模式的迭代演进，彻底改变了网络连接的核心使命，推动网络连接层从单纯的数据传输通道，升级为异构智能体协同交互的标准化、可容错、可扩展、高安全的公共互联平台。

从互联网产业迭代历程来看，应用架构的解耦与开放化演进，是智能体网络连接层诞生的核心底层动因，完整经历了紧耦合单体架构、松耦合微服务架构到开放互联智能体架构的三次范式变革，对应网络连接能力的逐级升级。Web互联网时代以浏览器为终端载体，基于TCP/IP协议构建B/S架构体系，应用普遍采用单一紧耦合的单体架构，将应用前端、业务逻辑与数据访问深度捆绑，整体系统封闭独立、边界清晰、交互逻辑简单。该阶段网络仅承担简单的网页数据请求与下发任务，应用无需跨主体协同，网络连接仅服务于固定的人机短时交互，不存在异构主体互联、动态组网与复杂任务协同的诉求，网络连接能力完全依附于基础IP传输能力，无独立的应用层连接治理体系。

移动互联网时代依托云计算、容器化与K8S编排技术，实现了应用架构的松耦合革新。传统单体应用被拆解为数十甚至上百个独立运行的微服务模块，各模块可独立开发、部署、迭代与扩容，模块之间通过私有API完成内部通信与业务联动。该阶段的解耦仅局限于单一厂商、单一系统内部，服务交互依赖私有化接口规范，跨平台、跨组织、跨系统的互通壁垒依然存在，应用网络整体仍呈现封闭化特征。网络连接主要承载数据中心内微服务调用、南北向业务访问，通信模式相对固定，连接关系静态可控，网络只需适配固定端口、固定接口的同步调用场景，无需应对动态、开放、自主的主体协同需求。

面向智能互联的网络时代彻底打破了传统应用的封闭边界，构建起全新的开放互联应用架构。随着MCP协议、A2A交互范式与自然语言Web体系的成熟，异构智能体、分布式数据资源与各类服务主体不再依赖私有接口与固定配置，而是通过标准化、开放化的公共协议实现全域互联。各类跨厂商、跨平台、跨组织、跨场景的智能体可自主接入网络、自由匹配协同资源，应用架构从系统内的松耦合，升级为全域开放的对等互联架构。应用架构的根本性变革，彻底颠覆了传统封闭、定制化的通信逻辑，传统基于私有API、固定连接、静态组网的网络连接体系已无法适配全域智能体协同需求，亟需一层独立的、标准化的公共互联基础设施，屏蔽异构智能体的技术差异，统一治理全域连接与通信行为，智能体网络连接层由此成为面向智能互联的网络的核心刚需层级。

除应用架构迭代外，智能体独特的长周期任务协同模式，彻底重构了网络通信机制，倒逼网络连接层重塑通信调度能力。传统Web与移动应用的通信具备典型的短时、同步、应答式特征，以毫秒级请求响应为核心交互逻辑，单次交互链路短、任务生命周期短、状态无留存，通信完成后连接即刻释放。而智能体通信以长任务协同为核心形态，多异构智能体围绕分钟级、小时级甚至天级的持续性任务开展深度协作，全程需要频繁共享任务上下文、开展多轮意图交互、自主协商分工与资源权益、动态调整组网关系。这种长周期、强状态、高联动的协同模式，对网络连接层的消息调度与分发能力提出了全新要求。

通信机制变化：从传统的同步阻塞到异步通信，黑板通信与订阅发布通信是智能体时代两类核心通信机

制，对网络连接层的消息调度与分发能力提出全新要求。黑板通信支持所有参与协同的智能体共享全局任务上下文，实现状态信息全域同步、实时可见，需要网络连接层提供统一的上下文存储与同步分发能力，保障多主体状态一致性。订阅发布模式则打破了传统点对点直连通信的绑定关系，消息发布者无需感知接收主体，仅基于主题通道推送消息，由订阅主体自主接收匹配信息。这就要求网络连接层承担全局消息中转站的核心职能，统一完成消息分类、主题路由、精准分发与异步投递，屏蔽智能体之间的交互耦合关系，实现消息传输的解耦化、异步化与精准化。

应用部署变化：传统应用均集中部署于大型云数据中心，具备稳定的网络传输、持续供电、充足算力与完善的基础设施保障，运行状态连续稳定，极少出现中途退出、链路中断等异常。而智能体具备泛在部署特征，可广泛部署于智能手机、个人PC、车载终端、具身机器人等各类泛在终端设备，普遍面临弱网络、低功耗、算力受限的运行环境，极易因网络波动、电量不足、设备休眠等因素临时退出协同任务。由于智能体任务具备超长周期特征，若因单个智能体临时离线导致整体任务中断、重启或失败，将造成极大的算力资源浪费，同时严重破坏用户体验。基于此，网络连接层需具备上下文消息缓存、任务状态持久化、离线消息暂存与上线断点续推能力，隔离单智能体动态上下线对全局任务的影响，保障长周期协同任务的连续性与稳定性，适配面向智能互联的网络不中断设计原则。

连接数量变化：智能体组网模式的迭代升级与连接规模的爆发式增长，推动网络连接层重构组网架构与连接管理模式。传统应用通信以固定点对点、客户端对服务器的连接形态为主，连接数量有限、拓扑静态、管理成本低。而智能体协同以多点Mesh组网、点对多点联动为核心形态，全域海量智能体可动态建立对等连接，连接规模呈指数级增长。若延续传统全连接Mesh组网模式，M个智能体与N个智能体协同将产生M×N组端到端连接，海量连接的建立、维护、保活将消耗巨额终端资源与网络资源，极易造成网络拥堵、终端算力过载。为解决海量连接治理难题，网络连接层通过代理网关实现组网架构革新，将传统全连接Mesh架构转化为星型代理架构，由连接层统一终结、转发所有智能体连接，将连接规模从M×N的指数级复杂度优化为M+N的线性复杂度，大幅降低终端连接管理压力与全网运维成本。该架构变革彻底释放了泛在终端的资源压力，同时实现了全网连接的统一管控、统一调度与统一容错，适配智能体海量、动态、短时、高频的连接特征。

交互模式变化：传统Web、移动APP均面向人机交互设计，依托可视化UI界面完成用户操作输入，全网寻址体系以URL资源定位为核心逻辑，通过固定地址、静态路径精准定位网页资源与服务接口，适配人类点击检索、主动拉取的交互习惯，寻址过程无语义理解、无任务意图匹配，仅为标准化资源定位动作。而面向智能互联的网络为纯机机自治协同模式，不存在人机交互UI界面，智能体之间不再依托传统URL、固定IP或接口地址完成寻址匹配，而是基于任务意图语义实现主动发现与精准对接。智能体以任务目标、能力诉求、协作意图为驱动发起交互，无需预设对方地址与服务入口，彻底颠覆了传统互联网标准化、结构化的资源寻址范式。在此背景下，智能体网络连接层新增语义寻址解析与智能体匹配核心能力，能够识别、解析智能体交互的任务语义与协同意图，基于能力维度、任务维度动态匹配最优协同智能体，实现无预设、无固定地址的语义化自主寻址。

综合上述架构、机制、场景与规模的多重变革，智能体网络连接层最终形成了Overlay叠加组网的核心架构形态，构建起区别于传统物理IP网络的全新应用互联体系。该层级部署于传统物理网络之上，不颠覆底层TCP/IP基础承载能力，而是通过标准化协议与公共互联能力，屏蔽底层物理网络差异、智能体异构差

异、部署场景差异，为跨平台、跨组织、跨域的海量异构智能体，提供安全可信、低时延、高并发、可扩展、可容错的专属通信网络。相较于物理网络层侧重带宽、时延、拓扑等基础资源承载，网络连接层更聚焦智能体业务协同逻辑，解决开放互联、异步通信、动态组网、断点续传、海量连接治理等新型核心问题。

总体而言，智能体网络连接层的核心作用，是承接应用架构从紧耦合、松耦合到开放互联的演进趋势，适配智能体长任务、异步协同、动态组网、泛在部署的全新特征，弥补传统物理IP网络面向人机短时交互、封闭固定连接、同步应答机制的能力短板。通过构建标准化Overlay公共互联基础设施，统一智能体通信协议、消息调度机制与组网治理模式，实现智能体通信解耦、状态可续、连接可控、全域互通，为上层智能体自主发现、自主协商、不间断协同、开放化交互提供核心连接支撑，是落地面向智能互联的网络开放互联、自主性、不中断、协作解耦四大设计原则的关键中间核心层级。

3.2.3 智能体网络管控层

网络管控层是面向智能互联的网络实现全域有序协同、可信治理、可管可控的核心中枢，位于网络连接层之上、智能体应用层之下，承担全网智能体身份治理、权限管控、状态管理、能力评估与策略调度的核心职能。传统互联网管控体系面向人机交互场景设计，以固定用户角色、固化应用功能、静态业务边界为治理前提，适配小规模、确定性、长生命周期的终端与业务形态。而面向智能互联的网络以海量自治智能体为核心主体，智能体具备生命周期短、行为概率化、任务边界不确定、动态组网迭代快等全新特征，同时未来全域智能体将达到万亿级规模，传统基于角色、静态配置、集中固化的管控模式已完全失效。在此背景下，网络管控层通过重构身份体系、管控架构与评价机制，构建适配海量、动态、不确定、自治化智能体场景的新型全域治理体系，为面向智能互联的网络自主协同、开放互联、稳定运行提供制度与策略保障。

传统互联网管控体系的核心逻辑是“以人为核心、以固定业务为边界”，具备极强的确定性与静态性。在Web互联网与移动互联网场景中，用户身份长期固定、角色权限清晰可定义，个人账号、设备终端的生命周期长、状态稳定。同时各类应用功能边界固化、业务逻辑固定、交互行为可预期，网络管控可依托固定角色权限、静态黑白名单、固化访问策略实现全域治理，认证鉴权、权限管控、状态维护的压力相对可控，整体治理模式简单、稳定、可落地。这种治理体系高度适配人类可控操作、固定业务交互的场景，但无法适配智能体自治协同的运行特征，存在根本性的体系性短板。

相较于传统人机交互场景，智能体的运行特征彻底颠覆了传统管控的前提假设，带来多重治理挑战。首先，智能体不存在固定身份角色与固化业务边界，其行为具备典型的概率性与不确定性。智能体依托大模型推理完成任务决策，同一智能体可根据不同任务场景、协作对象、环境状态产生差异化行为逻辑，业务边界随任务目标动态变化，无法用固定角色、固定权限、固定业务范围对其行为进行约束界定。其次，智能体生命周期碎片化、动态化，大量临时任务型智能体随任务创建、随任务销毁，在线状态频繁波动，上下线节奏远超传统终端设备，对全网状态实时同步、动态管控提出极高要求。

更为核心的是，未来面向智能互联的网络将承载近九千亿级别的海量智能体主体，超大规模体量对传统集中式注册、鉴权、状态更新体系形成颠覆性压力。传统互联网的集中式认证、统一鉴权架构，能够支撑千万级、亿级终端设备的运维管理，但无法承载万亿级智能体的高频注册、动态注销、实时状态同步、批量

权限更新需求，极易出现管控瓶颈、算力过载、同步时延过大、策略失效等问题。与此同时，传统网络缺乏针对智能体的能力评价与质量管控体系，仅能实现连通性与访问权限管控，无法对智能体的任务执行能力、协同可靠性、行为合规性、服务质量等级进行量化评估，难以支撑智能体自主择优协作、全网资源高效调度，无法保障复杂多智能体任务的整体执行质量。

为应对智能体不确定性行为、短生命周期、万亿级规模与无边界协同带来的多重挑战，面向智能互联的网络网络管控层构建了分层分域、集中管控+分布式执行的新型全域管控体系，实现治理能力的全方位升级。该体系突破了传统纯集中式管控的性能瓶颈与纯分布式管控的无序性缺陷，形成“顶层集中统筹、域内分布式同步、边缘就近执行”的分层治理架构。其中，集中式管控平面负责全网统一规则定义、全域智能体身份认证、全局权限鉴权体系搭建、跨域策略统筹与全网能力评级标准制定，保障全域治理规则统一、标准统一、权限统一，避免碎片化治理乱象。

分布式管控平面承担分域状态同步、局部策略迭代、域内智能体管理等轻量化能力，将海量智能体的状态更新、在线监测、局部权限调度下沉至各自治域，避免所有请求汇聚核心管控节点，彻底解决万亿级智能体注册鉴权、状态同步带来的性能压力。同时，网络管控层将策略执行能力下沉至边缘节点与网关层，实现权限校验、行为管控、流量治理、合规审计的就近执行，大幅降低管控时延，适配智能体高频动态变化的运行特征。这种分层分域的管控模式，既保留了集中式架构的规范性与统一性，又具备分布式架构的高并发、低时延、可扩容优势，完美适配海量、动态、跨域的智能体协同场景。

针对传统身份体系无法适配智能体匿名化、自治化、动态化交互的问题，网络管控层重构新型智能体数字身份体系（NHI），构建面向机机自治协同的全域可信身份底座。传统URL寻址、IP身份、用户账号身份均依附于人、依附于固定设备，身份与位置、设备、账号强绑定，无法适配智能体动态迁移、临时组网、无UI语义交互、短生命周期运行的特征。新型NHI智能体身份体系实现身份与物理位置、设备载体、固定账号的解耦，以智能体个体能力、可信属性、任务权限为核心标识，支持智能体动态注册、临时身份授权、周期身份销毁、跨域身份迁移。同时NHI身份内置可信校验机制，可适配智能体语义寻址、自主发现、动态协商的交互场景，为无预设、开放化的A2A协同提供可信身份支撑，解决了海量异构智能体跨域互联的身份可信问题。

在此基础上，网络管控层创新性构建智能体能力与质量量化评估体系，补齐传统网络无智能体治理能力的核心短板。传统网络仅关注网络传输质量，不关注业务主体能力，而面向智能互联的网络的核心是任务协同质量，管控层通过建立多维度评估指标体系，涵盖智能体任务完成率、协同可靠性、推理稳定性、行为合规度、资源履约能力、历史服务质量等核心维度，实现对全域智能体的动态打分、分级分类、信用评级。评估结果可实时应用于智能体自主匹配、全网任务调度、资源权限分配、异常主体限流管控，让网络管控从“权限准入的粗放管控”升级为“能力择优的精细化治理”，有效约束智能体概率性不确定行为，提升全网协同任务的整体成功率与稳定性。

综上，面向智能互联的网络网络管控层的核心功能与核心价值，是针对智能体区别于传统用户与应用的全新特征，解决不确定行为、短生命周期、万亿级规模、无边界协同带来的治理难题。通过搭建分层分域的集散融合管控架构、构建NHI新型智能体数字身份体系、建立智能体能力质量评估机制，实现全域智能体“身份可鉴、权限可控、状态可溯、能力可评、行为可管”。网络管控层有效承接了面向智能互联的网络

开放互联、自主协同、不中断、松耦合的架构特征，规范了海量自治智能体的无序交互行为，平衡了智能体自主协作与全网有序治理的关系，是面向智能互联的网络从“可连通”走向“可管控、高质量、高可信”的核心治理支撑层级。

3.2.4 智能体应用业务层

智能体网络的应用层是承接用户需求、承载智能体交互、落地业务能力的核心业务交互平面，区别于传统软件应用的功能执行层，其核心价值是通过标准化、智能化、动态化的节点连接，实现多智能体协同、工具资源调用、模型能力调用的全流程业务闭环。应用业务层聚焦业务交互与能力落地，承载所有智能体的业务交互、跨单元协同、资源调用、需求响应等核心行为。与传统分布式架构固定节点组网、固定流程执行的模式不同，多智能体系统应用层无固化拓扑结构，无中心化管控节点，所有智能体均为平等自治单元，可根据实时业务需求自主完成组网、协作、资源调用与任务收尾，具备动态自治、跨域协同、轻量化迭代的核心架构特征。

应用层的所有智能业务行为，均依托智能体单元与系统各类资源的交互连接实现。基于多智能体系统的业务运行逻辑，可推导得出应用层存在三类不可替代的核心交互连接，分别为智能体间协同连接、智能体–工具执行连接、智能体–模型认知连接。三类连接分别对应智能体的协同作业、业务执行、智能认知三大核心能力，覆盖需求响应全流程，构成应用层的基础交互拓扑。智能体间连接是应用层多单元协作的核心基础连接，核心作用是实现自治智能体之间的标准化通信、任务协同与能力互补。单一智能体的业务领域、认知范围、执行能力存在天然边界，无法独立完成跨领域、多环节、高复杂度的复合型业务，必须通过智能体间的互联交互，实现任务拆解、分工执行、结果聚合。

智能体到智能体：该连接具备标准化通信、全生命周期任务联动、动态组网三大核心特性。不同于传统系统自定义的零散接口交互，应用层智能体间遵循统一的消息格式、状态同步规则与任务交互逻辑，支持跨场景、跨领域智能体的无障碍通信，无需针对性开发适配代码。同时，连接覆盖任务从发起、执行、迭代到收尾的全生命周期，支持任务状态实时订阅、进度同步与异常反馈，可自主完成平等协商、方案迭代、冲突规避。在组网形态上，连接完全动态自适应，系统根据业务目标自动匹配最优智能体组合，临时构建协作拓扑，任务完成后自动解散组网，无需人工预设节点关联关系。

智能体到工具：智能体–工具连接是智能体实现业务落地、将认知决策转化为实操结果的能力延伸连接。智能体核心具备思考、规划、决策能力，但不具备具象化的业务执行、数据运算、场景操作能力，必须通过对接各类外置工具资源，补齐执行短板，形成“认知–决策–执行”的完整业务闭环。此处工具包含数据处理组件、办公服务、业务系统接口、物联网设备、第三方场景服务等各类可标准化调用的执行资源。该连接的核心特质是通用适配、按需调用、权限可控。应用层通过统一资源适配规范，将各类异构工具的调用逻辑、参数格式、返回结果进行标准化统一，让智能体无需适配不同工具的差异化接口，即可通用调用各类执行资源。业务执行过程中，智能体可自主识别当前环节的资源需求，精准匹配最优工具并发起调用，连接仅在任务执行窗口期生效，任务完成后自动释放资源，避免算力与接口资源冗余。同时，连接具备精细化权限管控能力，可界定不同智能体的工具调用范围、操作权限与调用频次。

智能体到模型：智能体–模型连接是智能体具备自主智能、区别于传统程序模块的核心底层连接。大模型与行业专用模型是智能体所有认知能力的算力源头，智能体通过常态化对接底层模型，获取语义理解、需

求拆解、逻辑推理、风险研判、内容生成等核心智能能力，是应用层所有智能化交互的基础前提。该连接具备能力赋能、动态迭代、算力最优调度的特性。模型为智能体提供分层智能支撑，通用模型保障基础交互与任务规划能力，行业专用模型提供垂直场景的精准决策能力。模型能力升级、微调优化后，可通过该连接同步赋能所有关联智能体，无需修改智能体自身逻辑代码，实现轻量化能力迭代。同时，应用层可根据业务任务的复杂度，通过该连接动态调度不同规格的模型算力，简单交互任务适配轻量模型降低算力消耗，复杂决策任务适配高精度模型保障服务精度，实现认知算力的高效利用。

面向智能互联的网络横向架构分层同时具备支撑异构智能体间，智能体到工具、智能体到模型的复杂连接、通信的需求与能力。

3.2.5 智能体网络安全

面向智能互联的网络全域自治协同、可信稳定运行的核心保障体系，区别于传统互联网分层独立、边界隔离、外挂部署的安全模式，智能体安全呈现典型的跨层联动、全域渗透、内生赋能的全新特征。传统互联网的安全以人机交互、固定业务、静态组网为基础前提，依托防火墙、入侵检测、权限管控等外挂式安全设备，基于网络边界实现集中式防御，可有效应对确定性的网络攻击与业务风险。而面向智能互联的网络具备跨层交互、Mesh动态组网、机机自主协同、长周期任务运行、语义化交互等全新特征，安全风险贯穿物理网络层、网络连接层、网络管控层与应用层全架构体系，同时衍生出模型、工具、数据、网络多维度新型攻击面。基于面向智能互联的网络的架构特征与全新安全风险，传统集中式、外挂式、边界式安全架构彻底失效，倒逼安全体系向网络内生、跨层协同、全链路、语义级动态防御演进，构建适配海量异构智能体自治协同的新型安全能力体系。

智能体安全风险具备极强的跨层渗透性与关联性，各层级架构均存在专属安全短板，且风险可跨层传导、叠加放大，决定了智能体安全必须依托跨层协同防御机制运行。在物理网络层，智能体泛在部署于云、边、端各类基础设施，无线网络、边缘节点算力功耗受限、防护能力薄弱，海量智能体动态上下线、大并发突发流量、上下行对等传输的特征，极易引发针对性的拒绝服务攻击、链路劫持、流量窃听，物理层基础设施的开放性导致网络边界彻底模糊，传统边界隔离防御完全失效。在网络连接层，智能体采用多点Mesh、点对多点的动态组网模式，连接关系动态迭代、无固定拓扑结构，海量智能体基于Overlay网络异步通信、断点续推、上下文共享，传统基于固定链路、静态连接的访问控制策略无法适配，链路伪造、消息篡改、上下文劫持、虚假节点接入等风险大幅提升。

在网络管控层，万亿级海量智能体短生命周期、概率性行为、无固定业务边界的特征，带来巨大的治理安全压力。海量智能体高频注册、注销、状态更新，集中式鉴权体系易出现权限滞后、策略失效问题，同时智能体无固定角色、行为不确定，静态权限配置、固定角色管控模式无法约束其动态协同行为，易出现越权协同、违规交互、身份冒用等安全隐患。在应用层，A2A自主协同、MCP语义化通信、长任务迭代运行的模式，催生模型、工具、数据多维度新型安全风险，攻击场景从传统网络流量攻击，延伸至语义攻击、逻辑攻击、业务攻击、数据投毒等高阶威胁。综上，智能体安全风险贯穿四层架构、相互关联影响，单一层级的安全防护无法实现全域可信，必须构建跨层协同的一体化安全体系，实现分层防护、全域联动、风险共治。

智能体Mesh化、多点对等连接的组网模式，彻底颠覆了传统安全的架构形态，推动安全体系从集中式外

挂防御向分布式内生安全全面演进。传统互联网以云数据中心为核心，采用中心化C/S架构，流量南北向集中收敛，安全防御依托核心节点外挂安全设备，通过集中检测、统一拦截实现全域防护，具备防御范围固定、策略静态、运维集中的特征。而面向智能互联的网络摒弃了中心化调度模式，大规模采用Mesh多点组网、点对点动态协同、边缘就近交互模式，东西向流量占比大幅提升，流量分散、拓扑动态、交互自由，无固定流量收敛中心。

在此架构下，传统集中式安全网关无法覆盖全域流量，外挂式安全设备存在防护滞后、策略脱节、适配性差等问题，无法适配智能体动态组网、自主协商、无预设交互的运行特征。同时，智能体自主协同无需人工干预，安全决策、风险拦截、权限校验需要实时、动态完成，外挂式后置防御模式无法满足实时防护需求。因此，智能体安全架构必须重构为网络内生安全体系，将安全能力原生嵌入物理网络、连接传输、管控治理、应用协同全流程，让安全策略随组网动态迭代、安全能力随连接实时生效、安全管控随任务全程覆盖，实现“组网即安全、传输即防护、协同即可控”，彻底适配Mesh化全域对等协同的架构特征。

相较于传统互联网，面向智能互联的网络新增模型、工具、数据三类核心攻击暴露面，叠加传统网络安全风险，形成全链路、多维度的复合型安全威胁体系，对全域防护能力提出极致要求。首先是智能体模型层安全风险，作为智能体自主决策、意图识别、任务执行的核心底座，模型自身存在诸多原生安全隐患。一是提示词注入攻击，攻击者通过构造恶意语义、嵌套引导指令，绕过智能体原有约束规则，引导智能体执行越权操作、泄露隐私数据、生成违规内容；二是模型藏毒与非预期接口风险，异构智能体模型在训练、迁移、部署过程中可能被植入隐性非预期接口与恶意逻辑，正常运行时无异常，特定场景下触发恶意行为，引发隐蔽式安全事件；三是过度代理风险，智能体具备自主决策、自主执行能力，易出现权限滥用、行为越界、过度替代用户与系统执行高危操作的问题，引发不可控的业务与安全风险。

其次是智能体工具调用安全风险，智能体依托MCP协议调用各类第三方工具、API、外部服务完成协同任务，工具开放调用模式带来全新安全漏洞。一是越权访问风险，智能体动态决策过程中可能突破权限边界，违规访问受限数据、涉密接口与隐私资源；二是恶意资源访问风险，智能体自主检索、联网调用过程中，可能主动访问恶意网站、钓鱼链接、恶意服务，引入病毒、木马与违规资源；三是MCP工具非预期接口与API恶意调用风险，第三方工具与接口存在预置非预期接口，攻击者可通过恶意调用、参数篡改，窃取智能体上下文数据、劫持任务执行流程；四是资源滥用风险，恶意智能体可通过高频调用、批量请求，快速消耗网络带宽、云端算力、接口配额等公共资源，引发资源枯竭与服务瘫痪；五是执行参数篡改风险，攻击者可篡改智能体工具调用参数、任务执行指令，引导智能体执行违规操作，破坏任务完整性与正确性。

再者是智能体数据层安全风险，智能体长周期任务协同、多轮语义交互、记忆存储机制，导致敏感数据暴露面大幅扩张。智能体在协同过程中会持续采集、处理、流转企业业务数据、用户个人隐私数据，其专属的长期记忆、短期记忆与向量数据库会批量留存各类敏感信息，若缺乏防护极易引发数据泄露、滥用、篡改风险。同时，海量智能体跨域、跨平台、跨区域协同，会导致敏感数据全域流转，极易出现数据跨境传输违规、数据溯源困难、数据流转失控等问题，违反数据安全与个人隐私保护规范，引发合规风险与信息安全隐患。

最后是传统网络安全风险的迭代升级，适配智能体全新场景衍生新型威胁。一是账号与凭据窃取风险，海

量智能体动态接入、匿名协同，身份凭据易被窃取、伪造、冒用，引发非法接入、虚假协同问题；二是模型文件盗取风险，智能体模型、配置文件、专属知识库具备极高价值，易成为重点攻击目标，出现非法窃取、复制、篡改等行为；三是拒绝服务攻击升级，攻击者可利用智能体高并发、强突发的流量特征，发起针对性流量攻击，占用网络与算力资源，导致多智能体协同任务中断、全网服务瘫痪。

针对上述全链路、多维度的新型安全风险，智能体内生安全体系衍生出三大核心刚需能力，实现对智能体专属威胁的精准防护与全域管控。

第一，语义级攻击识别与防护能力。区别于传统网络基于特征、规则的流量检测模式，智能体安全需要深度解析MCP协议封装的语义信息、任务意图、交互内容，精准识别提示词注入、语义引导、隐性攻击等新型高阶威胁，实现从“特征匹配防护”到“语义理解防护”的升级，拦截各类模型语义层恶意攻击，守护智能体决策与交互安全。

第二，动态语义级最小权限授权能力。针对智能体行为不确定性、任务动态性、组网灵活性的特征，摒弃传统静态角色授权、固定权限分配模式，基于智能体实时任务意图、协同场景、能力诉求，实现动态、细粒度、语义化的权限按需授予与回收。严格遵循最小权限原则，仅为智能体开放当前任务所需的最小资源与操作权限，任务结束即时回收权限，杜绝越权访问、过度代理、权限滥用风险，适配智能体动态协同的安全管控需求。

第三，全链路数据隐私防泄漏能力。覆盖智能体数据采集、语义交互、工具调用、记忆存储、跨域流转全流程，构建隐私脱敏、访问审计、流转追溯、异常拦截机制。针对智能体短期记忆、长期记忆、向量数据库的敏感数据，实现加密存储、权限隔离、脱敏使用，同时监测跨域数据流转行为，拦截敏感数据外泄、违规出境等行为，实现智能体数据全域可控、可溯、安全可用。

3.2.6 智能体网络可观测

可观测性是面向智能互联的网络实现全域可控、可评、可优化、可溯源的核心运维与治理底座，是区别于传统网络运维体系的关键能力升级。传统互联网可观测性聚焦物理网络设备、链路质量与业务访问状态，以网络时延、丢包、带宽、设备在线率等基础指标为核心，仅能实现网络底层资源的状态感知，无法适配智能体自主协同、任务化交互、动态组网、概率性行为的新型运行特征。面向智能互联的网络以全域异构智能体的长周期自治任务协同为核心业务形态，业务流程跨物理网络层、网络连接层、网络管控层与应用交互层，行为具备不确定性，任务具备突发性，资源消耗具备动态性。传统单点、分层、静态的监测体系已无法实现全域状态感知，亟需构建覆盖全链路维度、涵盖多维可视指标、支持分域自治与跨域协同的新型智能体可观测体系，为智能体任务调度、质量优化、风险治理、成本管控提供核心数据支撑与决策依据。

智能体可观测性首先突破传统网络单层观测局限，构建物理层、连接层、应用交互层全链路一体化可观测体系，实现从“网络可视”到“业务全链路可视”的范式升级。在物理网络层，可观测性聚焦云、边、端全域基础设施资源状态，核心覆盖数据中心与边缘节点的算力负载、存储占用、上下行带宽利用率、无线信道冲突、链路时延抖动、设备在线状态等基础物理资源指标，实现对智能体承载底座的资源余量、传输质量、运行负荷的实时感知，解决智能体大上行流量、高并发突发流量带来的网络拥塞、资源瓶颈难以预

判的问题。物理层可观测是全域智能体稳定运行的基础保障，能够精准定位底层网络传输、硬件资源、无线调度带来的任务执行异常。

在网络连接层，可观测性聚焦智能体Overlay组网与A2A通信过程，适配Mesh动态组网、多点对多点连接、异步消息交互、断点续推的运行特征。其观测内容涵盖智能体动态上下线状态、组网拓扑变化、节点连接数量、消息发布订阅状态、上下文同步进度、链路存活时长、消息投递成功率等连接维度指标。相较于传统网络仅关注固定链路连通性，连接层可观测能够精准捕捉智能体动态组网过程中的连接震荡、消息丢失、同步超时、组网异常等问题，适配智能体无预设、动态化、松耦合的协同模式，实现对智能体通信链路全过程、全状态感知。

在智能体应用交互层，可观测性聚焦智能体任务化、意图驱动的业务协同过程，突破传统应用请求响应的单一观测维度。重点覆盖多智能体任务拆解、分工协商、迭代交互、进度执行、结果交付、异常重试、任务中断与接续等业务全流程状态，同时观测MCP协议语义交互、意图匹配、多轮对话协同、智能体自主决策等上层交互模式。应用层可观测实现了从“看网络通断”到“看任务成败”的核心升级，能够精准识别智能体概率性行为、决策偏差、协同适配不足等新型问题，真正贴合面向智能互联的网络以任务执行为核心的业务本质。

基于全链路可观测底座，面向智能互联的网络进一步构建**质量可视、行为可视、成本可视**的多维一体化观测能力，覆盖智能体运行、协同、运维的核心治理维度。首先是协同质量可视，聚焦多智能体任务执行效果，建立任务完成率、执行时延、协同成功率、断点接续稳定性、语义匹配准确率、异常失败率等核心质量指标，全面量化智能体协同服务质量，解决传统网络无法评价智能体业务履约能力的短板。其次是智能体行为可视，针对智能体自主决策、自主协商、动态组网的特征，观测智能体接入行为、协商行为、工具调用行为、数据交互行为、上下线行为、越权异常行为等，实现机机交互行为的全程留痕、动态感知、异常预警，约束智能体不确定性概率性行为。

再次是资源成本可视，智能体协同涉及算力、带宽、存储、接口调用等多维资源消耗，传统网络缺乏精细化成本统计能力。智能体可观测体系能够实现单智能体、单任务、单协同链路的资源消耗精准统计，量化云端算力成本、边缘资源占用、网络带宽开销、工具调用损耗等，支撑全域资源精细化管控与成本优化。质量、行为、成本三维可视能力，彻底改变了传统网络“只看状态、不看质量、不看行为、不算成本”的粗放式运维模式，实现智能体协同全维度、精细化、数字化治理。

多维度、全链路化观测能力的落地，面向智能互联的网络必须建立**统一的可观测Benchmark与标准化评价体系**。传统互联网观测指标零散、标准不统一，不同厂商、不同架构、不同场景的设备与应用指标体系相互独立，无法形成全域横向对比、统一评价与全域调度依据。而面向智能互联的网络具备海量异构、跨域协同、开放互联的特征，不同类型智能体的执行能力、协同质量、资源消耗差异极大，若无统一的观测基准与评价标准，将导致智能体能力无法量化、任务调度无依据、异常判定无标准、质量优化无方向。

因此，智能体可观测体系需要统一指标定义、统一采集规范、统一评分基准、统一告警阈值与统一质量评级标准，构建面向智能体协同的标准化Benchmark体系。通过标准化基线，可实现全域智能体能力评级、质量对标、成本对标、异常对标，为智能体自主择优协同、全网任务调度、资源动态分配、异常智能体淘汰治理提供量化依据，解决海量异构智能体协同质量参差不齐、治理标准碎片化的核心问题。

针对面向智能互联的网络跨域组网、全域协同、海量节点的运行特征，智能体可观测体系最终形成**分域自治、跨域整合**的分层协同观测架构，实现观测效率与全域一致性的统一。万亿级智能体全域部署、跨域动态协同，若采用传统集中式统一观测模式，会产生海量观测数据汇聚，造成核心管控节点算力过载、数据同步时延过大、观测实时性不足，无法适配智能体高频动态变化的运行特征。因此，可观测体系采用域内自治观测模式，各智能体自治域独立完成本域内智能体的状态采集、指标统计、异常研判、数据存储与本地运维治理，实现轻量化、低时延、高实时的域内观测能力，分担全域观测压力。

在分域自治的基础上，通过跨域数据汇聚、标准统一、全域关联分析，实现跨域整合能力。各自治域按照统一观测标准向上汇聚核心指标、异常事件与质量数据，全网管控平面完成跨域数据关联、全域拓扑分析、跨域协同质量研判、全局资源调度评估，实现“域内精细自治、全域宏观统筹”。该架构既解决了集中式观测的性能瓶颈，又规避了分布式观测的碎片化问题，完美适配面向智能互联的网络分层分域、开放自治、全域协同的架构特征。

综上，智能体可观测性体系的核心功能与架构价值，是构建覆盖物理层、连接层、应用层的可观测能力，通过质量、行为、成本多维可视，结合统一标准化观测基准与分域跨域协同观测架构，实现海量异构智能体“状态可感知、行为可追溯、质量可量化、成本可精细化、异常可预警”。可观测性体系作为面向智能互联的网络治理体系的重要支撑，有效适配智能体不确定性、动态性、长周期、大规模的协同特征，为智能体自主掌握、高质量、高效率的全域自治协同提供数字化、标准化、智能化的运维治理保障。

3.3 面向智能互联的网络协议体系

智能体网关作为实现异构智能体跨域互联的基础设施，需要构建一套完整、标准化的协议体系，以支撑智能体在全生命周期内的注册、发现、同步与通信。该协议体系是智能体网关实现互联互通、安全可控、高效协同的技术基石。具体包括以下三大类核心协议：

- 智能体注册发现协议
- 智能体元数据同步协议
- 智能体消息传输协议

（1）智能体注册发现协议

智能体注册发现协议是智能体网关实现资源统一管理与精准寻址的基础协议，涵盖智能体从接入到退出的全生命周期管理。该协议定义了以下关键能力：

- **智能体身份标识分配**：为每个接入系统的智能体分配全局唯一的身份标识（Agent ID），确保标识的唯一性、不可伪造性与可追溯性。
- **智能体身份认证**：基于零信任安全架构，实现智能体与网关之间的双向身份认证，确保接入智能体的身份真实可信，防止身份伪造与中间人攻击。
- **智能体元数据注册**：定义标准化的元数据格式与注册流程，智能体在接入网关时，需提交包括能力模型、接口规范、运行状态、服务等级、信任等级及部署位置等核心元数据。网关对元数据进行校验、

存储与索引，构建全局动态资源库。

- **智能体发现**：支持基于语义级匹配的智能体发现机制，上层业务可根据功能属性、实时状态、负载能力、地理区域等多维条件，精准查询并匹配目标智能体。发现过程支持同步与异步两种模式，满足不同场景的时效性要求。

该协议确保智能体在分布式、多域环境下的高效注册与精准发现，为跨域协同调度提供准确、实时的资源视图。

（2）智能体元数据同步协议

智能体元数据同步协议用于实现多网关之间的高效、安全元数据同步，是保障分布式网关集群中资源信息一致性的核心技术手段。该协议定义了以下关键能力：

- **增量同步机制**：支持基于版本号、时间戳或事件序列的增量同步策略，仅同步发生变更的元数据项，避免全量同步带来的带宽与计算开销，显著提升同步效率。
- **事件驱动传播**：当某一网关域的智能体元数据发生变更时，变更事件以事件驱动方式触发同步，通过发布–订阅机制或协议在毫秒级时间内传播至全网其他网关节点，确保资源信息的实时一致性。
- **安全同步通道**：网关之间的元数据同步通道采用端到端加密与双向认证机制，防止元数据在传输过程中被窃取、篡改或伪造，保障同步过程的安全性与完整性。

该协议确保多网关环境下智能体元数据的一致性与实时性，为跨域寻址与任务调度提供准确、可靠的数据基础。

（3）智能体注册发现协议

智能体消息传输协议用于实现智能体之间通过智能体网关进行可靠、安全、高效的通信，是支撑多智能体协同作业的核心数据通道。该协议定义了以下关键能力：

- **点对点通信**：支持任意两个智能体之间的端到端消息传输，网关负责消息的路由、转发与投递。支持文本、二进制、流式等多样化数据负载，满足不同业务场景的传输需求。
- **群组通信**：支持基于群组的单播、广播与组播通信模式。智能体可根据业务需求加入或退出群组，网关负责群组成员管理、消息复制与分发。群组通信支持动态成员变更与消息顺序保障，适用于多智能体协作、状态同步等场景。
- **通信加密**：支持TLS加密与群组加密。TLS加密保障网关与智能体之间的通信通道安全。针对群组通信场景，支持基于群组共享密钥或公钥加密的群组消息加密机制。群组成员使用群组密钥加密消息，非群组成员无法解密。
- **端网协同**：支持智能体端与网络侧的协同优化机制。智能体可向网关上报网络状态与传输需求（如带宽、时延、可靠性要求），网关根据网络状况动态调整路由策略与流量控制参数，实现端到端的网络感知与自适应优化，提升消息传输效率与服务质量。

该协议为多智能体协同作业提供灵活、安全、高效的通信基础设施，满足从简单点对点消息到复杂群组通信、从普通数据传输到高安全等级加密传输的多样化需求。

通过构建这一标准化的协议体系，智能体网关得以在异构、多域、大规模部署环境中，为智能体提供高效、安全、可靠的互联通信能力，成为多智能体协同生态的核心基础设施。

4 智能体网关核心功能

智能体网关是面向智能互联的网络的核心转发与管控枢纽，承担全域智能体接入互通、协同调度、安全治理、运维观测核心职责，是实现异构智能体大规模跨域协同的关键基础设施。其技术能力体系由全域互联接入、智能体业务体验保障、智能互联安全防护、全域运维可观测四大能力构成，覆盖智能体入网、交互、执行业务、安全管控、运维运营全流程，形成可落地、可工程化、可规模化的技术支撑体系。

4.1 全域互联接入能力

全域互联接入能力为智能体网关基础底座能力，面向异构智能体多协议、多架构、分布式部署特征，解决协议不互通、资源不可见、跨域不同步问题。通过协议统一转换、智能体资源注册发现、跨智能体网关元数据同步机制，实现海量智能体低时延、高并发接入与转发，支撑全域组网互通。

图 6 智能体网关的连接与接入功能

（1）智能体注册与精准发现能力

针对多集群、跨地域分布式智能体部署场景，智能体网关提供标准化智能体注册与动态发现能力。入网智

能体统一上报能力模型、接口信息、部署位置、运行状态、负载指标、服务等级等元数据，智能体网关构建实时更新的全域智能体注册表，支持万级并发智能体注册接入，满足大规模集群上线场景。

在智能体发现层面，智能体网关摒弃传统IP寻址模式，采用基于业务意图、智能体功能标签、实时负载、区域位置的语义化寻址机制，实现多维权重最优节点匹配。整体寻址时延维持在毫秒级，支持高频次、大规模智能体调用与协同调度。

（2）分布式网关智能体元数据快速同步能力

多智能体网关分布式部署场景下，各域智能体网关独立管理本地智能体资源，易形成域内资源视图隔离。智能体网关定义标准化智能体元数据，作为智能体全域统一身份与能力描述载体，包含唯一标识、接口规范、运行状态、可信等级、服务约束等核心元数据。

多智能体网关集群采用事件驱动增量同步机制，仅同步智能体上下线、状态变更、负载波动等增量数据，无需全量同步，降低带宽开销。跨智能体网关元数据同步时延达到亚秒级，配套失效智能体自动淘汰、离线状态同步机制，保障全网智能体资源视图一致性，支撑跨域、跨企业、跨集群大规模智能体协同调度。

（3）跨协议高速互通能力

当前行业内智能体产品架构各异，通信协议标准尚未统一，协议生态碎片化已经成为制约多智能体集群规模化协同发展的主要瓶颈。智能体网关搭载高性能协议解析与双向转换引擎，搭建统一标准化通信适配平面，全面兼容 REST、gRPC、MCP、A2A 等行业主流智能体交互协议，同时适配同步通信、异步推送、流式数据交互等多元化业务通信形态。

网关可自主完成异构通信报文快速解析、业务语义统一映射、数据格式标准化转译与高效封装转发，在不改动存量智能体业务代码与现有运行架构的前提下，实现异构智能体之间无感无缝对接。依托硬件级转发加速机制，有效提升异构协议报文整体转发吞吐量、转发效率与运行稳定性，彻底隔离底层通信协议带来的使用差异，完成上层业务应用与底层通信网络的分层解耦，消除协议孤岛带来的集成阻碍，有效缩减多厂商、多生态智能体的集成对接成本与联调周期。

4.2 智能体业务体验保障能力

针对智能体长会话交互、链式协同、大模型推理交互等业务特征，传统网络扁平化调度无法匹配智能体差异化业务需求。智能体网关从智能体业务分级、网络态势感知、带宽资源预留、SRv6确定性传输四个维度，构建面向智能体业务的端到端QoS保障能力，提升跨域协同的传输稳定性与业务确定性。

图 7 智能体网关业务体验保障功能

（1）Agent业务网络需求精准分类

智能体网关基于业务交互特征、时延敏感度、可靠性要求与任务优先级，对全网智能体业务进行分级分类，覆盖大模型推理交互、多智能体链式协同、实时指令调度、离线批量任务、边缘联动业务等典型场景。针对不同业务识别其带宽、时延、抖动、丢包、会话保活等差异化网络诉求，为精细化QoS调度提供业务基线依据。

（2）面向Agent业务的全网网络态势感知

智能体网关实时采集全网骨干链路、分支链路、边缘接入链路的时延、抖动、丢包、带宽利用率、路由状态等网络指标，形成全域网络态势视图。同时感知智能体业务会话状态、跨节点调用链路质量、业务传输损耗，可提前识别链路拥塞、路由震荡、传输质量劣化等风险，为动态流量调度与路径优化提供实时数据支撑。

（3）智能体业务专属网络带宽资源预留

智能体网关支持基于业务SLA等级与任务优先级的静态、动态资源预留，对核心智能体实时协同业务、高等级推理任务分配专属带宽与上下行传输配额。通过流量优先级隔离机制，隔离核心业务与普通业务、低优先级批量流量，杜绝资源抢占，保障关键智能体业务传输带宽稳定。

（4）智能体业务承载优化

针对跨域、跨集群广域智能体协同场景，智能体网关可以基于SRv6分段路由等技术构建专属确定性传输通道。利用SRv6路径可编程、端到端切片、业务精准引流等能力，为跨域智能体协同业务规划最优传输路径，降低跨网转发时延与路由抖动。同时支持故障链路快速切换、流量无损迁移，在链路拥塞、节点故障场景下保障长会话智能体业务不中断，提升广域协同业务的传输可靠性与确定性。

4.3 智能体业务体验保障能力

针对智能体长会话交互、链式协同、大模型推理交互等业务特征，传统网络扁平化调度无法匹配智能体差异化业务需求。智能体网关从智能体业务分级、网络态势感知、带宽资源预留、SRv6确定性传输四个维度，构建面向智能体业务的端到端QoS保障能力，提升跨域协同的传输稳定性与业务确定性。

图 8 智能体网关的安全防护功能

（1）统一身份认证与入网接入管控

智能体网关为所有入网智能体分配全局唯一身份标识，支持数字证书、非对称密钥、可信令牌等多种认证方式，实现智能体网关与智能体双向身份校验。基于白名单准入机制执行接入管控，仅认证合法、有效的智能体可入网通信，从接入层拦截非法节点、身份伪造、仿冒接入等风险。

（2）任务级动态精细化权限管控

智能体网关摒弃静态授权模式，基于任务类型、安全等级、执行上下文动态生成最小权限集。智能体仅拥有当前任务所需的调用、访问与操作权限，任务结束或会话超时后自动回收临时权限，有效避免权限滞留、越权访问与权限滥用，实现权限全生命周期动态治理。

（3）智能体专属业务威胁与异常行为防护

智能体网关内置智能体业务安全风控引擎，可识别并拦截Prompt注入、恶意指令引导、协同劫持、异常高频调用、越界资源访问等智能体专属攻击行为。实时监测全网智能体调用频次、交互行为路径、会话状态，基于业务行为基线识别异常，自动执行限流、熔断、阻断、告警等处置策略，实现业务风险全链路防御。

（4）全链路安全行为审计与溯源追溯

智能体网关全量留存智能体认证记录、权限变更、跨节点调用、异常行为、风险处置等日志，采用防篡改存储机制，保证日志不可抵赖、不可篡改。支持按智能体ID、任务、时间、风险类型多维度检索复盘，可快速定位安全事件根因、追溯行为链路、界定责任，满足政企合规审计与安全治理要求。

4.4 全域可观测能力

针对分布式智能体组网普遍存在的运维黑盒、故障定位难、资源管控弱等痛点，网关搭建一体化多层级可观测体系，实现全网运行状态全方位可视化监测、故障精准定位、态势量化分析，支撑大规模智能体网络精细化、自动化运维。

图 9 智能体网关的全域观测功能

（1）智能体通信网络态势观测

网关自动探测全网网关节点、智能体集群及跨域互联链路，生成完整组网拓扑视图，直观呈现节点分布、链路连接关系与骨干路由架构。同时常态化采集全网各类链路时延、抖动、丢包率、带宽利用率、传输损耗等核心网络指标，完成链路质量量化评级，及时识别拥塞链路、劣质链路与网络异常状态，为路由优化、流量调度与网络运维提供完整数据依据。

（2）智能体节点运行状态观测

统一采集接入智能体的在线状态、服务运行状态、硬件负载、资源使用率、会话连接数、调用成功率等运行指标，实现单节点与集群状态集中监测。可及时发现节点离线、服务异常、负载过高、会话堆积等故障，实现异常提前预警。

（3）跨智能体业务交互观测

针对多智能体协同业务，端到端监测业务调用链路、响应时延、会话时长、调用成功率、任务完成率、异常终止率等业务指标。完整还原协同业务调用链路，精准定位交互超时、链路卡顿、流程中断等业务故障点，提升业务问题排查效率。

（4）网络安全运行态势观测

汇聚全网接入审计、权限操作、攻击拦截、异常行为等安全日志，对接国家监管平台，构建统一安全态势看板。量化展示攻击频次、异常接入、违规调用、高危风险分布，支持安全趋势分析与态势预警，支撑网络安全策略迭代与风险治理。

5 智能体广域网络

智能体时代的到来，并非仅仅是网络上应用形态的简单增加，而是对网络基础架构本身的一次范式重构。广域网的角色和其承载的流量特征正在发生两个根本性的、不可逆转的变化。

5.1 智能体广域网络应用业务场景

本章重点介绍智能互联广域网络在真实业务场景的落地实践，其中家庭场景包含智慧康养场景、跨家庭协同场景、金融行业场景作为重点案例深入展开。

5.1.1 家庭场景1–居家康养

随着医学进步与生活水平提升，全球人口结构正发生深刻变革，老龄化已成为 21 世纪最突出的社会特征之一。养老压力持续攀升的背景下，传统家庭养老受家庭结构小型化、子女异地就业、照护时间不足的制约愈发明显；机构养老则存在供给缺口大、成本高昂、老人归属感与接受度低等问题，两者均面临严峻挑战。居家养老是全球老年人的主流养老选择，但其照护需求的刚性与家庭供给能力的缺口正持续扩大。国家统计局数据显示，2025 年末我国 60 岁及以上人口达 3.23 亿，占总人口 23%，正式进入深度老龄化社会；我国长期保持 “9073” 养老格局，90% 老年人选择居家养老、7% 社区养老、3% 机构养老。2026 年居家养老服务市场规模将达 4914 亿元，智慧康养细分领域年增速超过 20%，是万亿银发经济中刚性最强、渗透率提升空间最大的赛道。智慧康养凭借信息技术赋能居家场景，成为破解居家养老难题的核心路径。同时我们从当前智慧家庭方案与市场中，呈现出一种矛盾的景象：智能设备数量激增，但家庭的整体“智慧”水平并未实现质的飞跃。设备功能独立、数据互不相通、生态系统壁垒高耸，形成了大量的“智能烟囱”，严重制约了真正个性化、主动式、协同化的真正的智慧家庭实现。

5.1.1.1 场景背景与需求分析

随着医学进步与生活水平提升，全球人口结构正发生深刻变革，老龄化已成为 21 世纪最突出的社会特征之一。养老压力持续攀升的背景下，传统家庭养老受家庭结构小型化、子女异地就业、照护时间不足的制约愈发明显；机构养老则存在供给缺口大、成本高昂、老人归属感与接受度低等问题，两者均面临严峻挑战。居家养老是全球老年人的主流养老选择，但其照护需求的刚性与家庭供给能力的缺口正持续扩大。国家统计局数据显示，2025 年末我国 60 岁及以上人口达 3.23 亿，占总人口 23%，正式进入深度老龄化社会；我国长期保持 “9073” 养老格局，90% 老年人选择居家养老、7% 社区养老、3% 机构养老。2026 年居家养老服务市场规模将达 4914 亿元，智慧康养细分领域年增速超过 20%，是万亿银发经济中刚性最强、渗透率提升空间最大的赛道。智慧康养凭借信息技术赋能居家场景，成为破解居家养老难题的核心路径。同时我们从当前智慧家庭方案与市场中，呈现出一种矛盾的景象：智能设备数量激增，但家庭的整体“智慧”水平并未实现质的飞跃。设备功能独立、数据互不相通、生态系统壁垒高耸，形成了大量的“智能烟囱”，严重制约了真正个性化、主动式、协同化的真正的智慧家庭实现。

1.老人康养场景：多设备功能独立碎片化，无协同闭环短板尤为凸显

在对连续性、闭环性要求极高的家庭康养场景，“智能烟囱” 的弊端被充分暴露，单一独立设备无法构建有效安全防护网，典型设备与智能体的局限如下：

- 光感雷达监测设备独立状态下可实现老人跌倒检测、人体存在感知、活动行为路径记录与久坐提醒。但协同能力完全缺失：检测到跌倒异常后，不能自动联动智能门锁解锁、同步开启公共区域照明为救援铺路，也无法联动可穿戴设备调取实时生命体征、触发急救服务呼叫；无法联动智能药盒判断异常倒地是否由漏服降压药等药物引发，仅能输出单一的跌倒告警信号，缺乏上下文信息支撑救援决策。
- 智能门锁独立状态下支持指纹、密码、远程临时密码开锁，具备防撬、试错告警能力。但在康养场景中存在明显协同盲区：无法结合光感雷达的居家活动数据，对 “老人超过 24 小时未出门、长时间未触发开门记录” 等异常状态主动预警；急救场景下无法与跌倒检测设备联动自动解锁，仍需人工远程操作或老人自行开门，延误黄金救援时机；也无法为陪护机器狗、社区养老上门服务人员自动分配临时出入权限，权限管理完全依赖人工手动配置。
- 家庭助手智能体独立状态下可实现语音交互、用药提醒、日程管理、基础设备语音控制、生活信息查询等功能。但作为家庭语音入口无法打通跨生态设备能力：老人语音求助 “我头晕不舒服” 时，无法自动调用光感雷达的活动状态、可穿戴设备的体征数据、智能药盒的服药记录做综合风险判断，仅能机械拨打预设的子女电话；无法联动陪护机器狗完成近身查看、递送药品等指令，只能控制自身适配生态内的少量设备，无法成为家庭康养服务的统一调度入口。
- 一键呼叫紧急按钮完全依赖老人主动按压触发，突发昏厥、严重跌倒等丧失行动能力的场景下完全失效；仅能传递 “求助” 单一信号，无法同步跌倒位置、生命体征、屋内人员状态等现场信息，救援决策缺乏依据；呼叫发出后无响应验证，也无法联动门锁、照明、机器狗等设备辅助救援进场，无服务闭环。
- 智能药盒仅具备定时提醒、开盒记录功能，无法确认老人是否实际服药、服用剂量是否准确，也无法排除宠物误食等异常；不能与血压、心率等体征监测设备、光感雷达活动数据联动，当漏服药物引发身体指标异常、活动状态异常时，无法触发分级预警，也不能在服药后联动健康服务智能体评估药效。

- 视频看护摄像头依赖子女人工实时查看，存在信息过载与响应时差，风险事件往往发生在未查看的窗口期；即便发现异常，也受限于子女所处场景，无法第一时间联动机器狗近身查看、调度社区救援服务、解锁入户门禁，处置链路完全依赖人工串联。

图10 家庭多设备功能独立碎片化，无协同闭环短板尤为凸显

2.跨主体、多生态协同升级的核心挑战

家庭市场是运营商存量经营的核心基本盘，也是数字化转型背景下最确定的增长赛道。截至 2025 年底，我国家庭宽带接入用户达 5.83 亿户，普及率升至 117.9 部 / 百户。从运营商家庭康养来看，自有业务与外部均面临 OTT 服务商融入，要实现跨公司、跨生态协同与服务升级，面临2个核心挑战：

（1）运营商省公司康养个性化业务需求，个性适配开发与维护挑战大

家庭市场是运营商存量经营的核心基本盘，也是数字化转型背景下最确定的增长赛道。截至 2025 年底，我国家庭宽带接入用户达 5.83 亿户，普及率升至 117.9 部 / 百户。从运营商家庭康养来看，自有业务与外部均面临 OTT 服务商融入，要实现跨公司、跨生态协同与服务升级，面临2个核心挑战：

（2）运营商省公司基于自有优势业务，聚合外部生态提升业务能力的需求，对接开发维护是核心挑战

运营商集团自有康养平台擅长网络连接、设备接入、数据传输，但缺乏医疗专业资质、成熟康养终端产品、线下上门照护资源。信通院数据显示：全国居家康养硬件产品超过 4700 万台，65% 由第三方硬件厂商提供；互联网平台承接 70% 以上线上问诊、慢病科普、认知训练服务。省公司依靠内部优势资源，聚合OTT 服务商、头部硬件厂商、互联网平台都有自己的系统平台与生态的需求。不同生态方各自搭建独立后台系统，OTT 平台、硬件厂商、互联网康养平台均有私有协议，没有统一行业标准。跨生态每接

入一家厂商都要单独开发接口、做数据格式转换、联调测试，单个硬件厂商对接开发成本 15-30 万元，全省接入几十家生态伙伴，年度适配投入数百万元；省公司 IT 人员不足，接口修改、版本升级还需要集团审批，迭代周期长达 2-3 个月，无法快速适配业务推广节奏。即便完成接入，后期厂商固件版本升级，运营商平台也要同步适配，长期运维压力巨大。

5.1.1.2 场景解决方案

当前个人智能体与服务智能体正进入快速普及期：个人助理类智能体如 Hermes、OpenClaw，生活服务类智能体如小龙虾，以及健康管理、社区服务、应急救援等垂直领域服务智能体大量涌现；同时家庭内的光感雷达、陪护机器狗、智能药盒等智能设备，也可被抽象为具备感知、决策、执行能力的硬件智能体。智能体正在成为家庭场景中，设备、服务、应用的核心载体。

本方案基于分层、开放、协同的面向智能互联的网络架构，以家庭老人跌倒应急处置为核心验证场景，通过分布式部署的智能体网关构建独立的逻辑智能互联通信平面，打通家庭终端侧、A公司云、B公司云三类异构智能体的能力壁垒，实现 “边缘事件触发 - 语义寻址调度 - 多智能体协同验证 - 分级应急处置 - 全流程闭环审计” 的全自动应急响应。

方案联合运营商在现网节点部署验证，最小化设置 3 个智能体网关、3 类核心智能体，既验证面向智能互联的网络的跨域协同、可信接入、低时延调度等核心能力，也面向家庭康养场景打造可落地的差异化智慧家庭服务，打破传统智慧家庭的设备孤岛与生态壁垒。如下图所示。

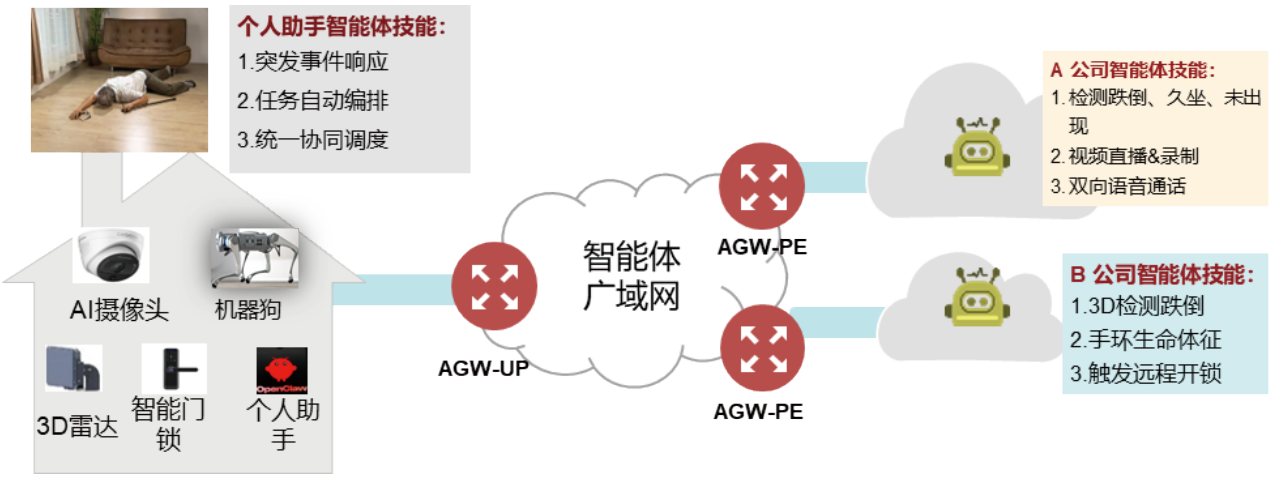


图11 家庭康养场景多智能体协同方案

（1）个人/家庭助手智能体（家庭智能体）

- 部署位置：家庭内智能体，采用PC部署
- 核心定位：家庭场景的智能体调度中枢与决策大脑，是家庭应急事件的第一响应主体
- 核心能力：
  - 突发事件应急响应与分级处置
  - 家庭全量智能体的能力盘点与动态画像

- 多智能体任务自动编排与协同调度
- 多源感知数据融合与应急决策
- 多渠道通知触达（家属、社区、急救机构）
- 全流程事件记录与复盘归档

（2）A公司智能体（视觉感知与交互载体）

- 部署位置：A公司云，对接家庭摄像头等视频设备
- 核心定位：家庭视觉感知能力的统一输出代理，提供视频类 AI 能力与音视频交互能力
- 核心能力：
  - AI 视觉事件检测：跌倒、久坐、长时间未出现、异常闯入等
  - 自定义标签检测与统计分析
  - 视频智能搜索、关键帧提取、事件摘要生成
  - 实时视频直播、云端录制与回放
  - 双向语音通话与语音广播

（3）B公司智能体（IoT 设备及各类服务）

- 部署位置：B公司云，对接家庭各类 IoT 与穿戴设备、娱乐、学习资源服务等
- 核心定位：家庭物联网设备能力的统一聚合代理，实现感知、穿戴、控制类设备的能力封装
- 核心能力：
  - 毫米波雷达跌倒检测与人员存在感知
  - 智能手环 / 手表生命体征采集（心率、血氧、血压、运动状态）
  - 触发智能门锁远程开锁确认与记录审计
  - 家庭内终端语音通知、多方通话能力

5.1.1.3 场景交互流程

场景目标：针对家庭老人跌倒的高危场景，通过多智能体协同实现 “秒级检测、快速验证、精准研判、分级处置、全程可溯”，解决单一传感器误报率高、应急响应链条长、跨设备协同难、上门救助安全风险高等痛点，保障老人黄金救援时间，同时兼顾家庭隐私与安全。全流程协同步骤，整个应急流程分为 6个阶段，全程由智能体自主协同完成，无需人工干预，高危环节支持human-loop确认。

步骤0：智能体上线、注册发布

1.自动向就近的网关注册能力，获取身份信息；智能体网关之间根据家庭统一ID将订阅的服务智能体进行条件同步，建立智能体路由转发表；

步骤1：边缘事件触发与初始告警

1.感知触发：家庭客厅 毫米波雷达 7×24 小时实时监测，通过毫米波点云数据检测到人员跌倒异常，初步输出跌倒置信度、事件时间、发生位置等信息；

2.本地上报：毫米波设备将跌倒事件上报至B公司智能体，B公司智能体完成事件初步结构化封装；

3.跨网关事件寻址：B公司云智能体网关对事件进行合规校验后，将 “跌倒告警事件” 封装为标准语义事件，通过智能互联平面路由至对应家庭的家庭侧网关。

步骤 2：语义寻址与调度

1.事件接收与解析：家庭侧智能体网关接收到跌倒告警语义事件，解析事件类型、紧急等级、来源智能体等核心信息；

2.语义能力寻址：网关在本地注册的智能体能力库中，检索具备 “突发事件响应、任务编排调度” 能力的智能体，语义匹配寻址到家庭个人助手智能体；

3.低时延事件分发：家庭网关通过本地转发通道，将跌倒告警事件及来源信息毫秒级转发至个人助手智能体，同步触发应急响应流程。

步骤 3：个人助手智能体任务编排规划

1.可用能力盘点：个人助手智能体向家庭网关拉取当前在线、可用的全量智能体能力清单，确认A公司智能体（视觉确认）、B公司智能体（生命体征采集）等核心能力均可用；

2.应急预案匹配：加载家庭预设的跌倒应急处置预案，结合老人健康档案、紧急联系人信息等基础数据，生成多阶段协同任务流；

3.任务流设计：采用 “验证 – 研判 – 处置 – 闭环” 的四阶段串行架构，验证阶段采用并行调用模式压缩耗时。

步骤 4：多智能体协同验证（视觉 + 体征双确认）

个人助手智能体生成并行调用指令，通过家庭网关分发至A公司云网关与B公司云网关，两路验证同时执行：

1.A公司智能体视觉验证流程

- A公司云网关接收调用指令，完成身份校验、权限校验、合规校验，确认调用合法；
- 指令转发至A公司智能体，智能体根据跌倒位置调取对应区域的家庭摄像头，实时拉取现场画面；
- 运行高精度 AI 视觉算法进行二次确认，输出跌倒状态置信度、人员姿态、是否有意识回应、是否有自主活动能力等结构化结果；
- 自动提取现场关键帧、生成 10 秒事件视频摘要，随验证结果一并回传至个人助手智能体。

2.B公司智能体生命体征验证流程

- B公司云网关接收指令，完成安全校验后转发至B公司智能体；
- B公司智能体触发老人佩戴的智能手环 / 手表主动测量，实时采集心率、血氧、血压、跌倒冲击值等生命体征数据；
- 同步采集手环的位置信息、运动状态，确认人员是否处于静止状态；
- 将生命体征数据结构化处理后，回传至个人助手智能体。

3.关键特性：双模态交叉验证大幅降低单一传感器的误报率；并行调用将验证耗时压缩 50% 以上；网关层统一安全校验，避免非法调用家庭摄像头与隐私数据。

步骤 5：应急等级研判与分级处置

1.多源数据融合决策：个人助手智能体融合毫米波初判结果、视觉二次确认结果、生命体征数据，结合老人历史健康档案进行综合研判

2.三级分级处置机制

- 一级（误报排除）：视觉未检测到跌倒姿态、生命体征完全正常，判定为误报。自动结束流程，生成误报记录，同步优化毫米波检测阈值，不打扰用户；
- 二级（轻微跌倒，人员清醒）：确认跌倒事实，但生命体征平稳、人员可通过语音回应。执行以下处置：

  a.通过A公司智能体的双向语音功能，与老人对话确认状况，询问是否需要帮助；

  b.通过翼家智话向紧急家属发送语音通知 + 短信，向家属的个人智能体推送现场关键帧与位置信息；

  c.持续监测老人状态与生命体征，直至老人恢复正常活动。
- 三级（严重跌倒，高危状态）：确认跌倒，且伴随心率 / 血氧异常、人员无意识无回应、长时间无法起身等高危特征。执行紧急处置：

  a.自动拨打 120 急救电话，同步推送家庭详细地址、老人基础病史、过敏药物、现场关键信息等急救辅助数据（待实施）；

  b.向所有紧急联系人拨打电话 + 短信通知，同步向家属的个人智能体推送关键帧信息，开放临时现场视频流查看权限；

  c.向社区网格员与社区医院推送告警信息，请求就近上门支援（待实施）；

  d.持续监测生命体征，实时同步数据至急救端，为院前急救提供支撑。

步骤 6：社区/医护人员上门的触发远程人工确认开锁

针对急救人员、社区医护上门救助场景，通过多智能体协同实现安全、可信的触发远程人工开锁，解决老人倒地无法开门、家属不在场的痛点，同时保障家庭财产安全。

1.触发条件：急救人员 / 社区医护到达家门口，通过门口摄像头发起远程开锁申请；

2.当前考虑家属远程，发起家属语音通话，通过家属远程开锁；

3.触发远程开锁（Human-In-Loop）

- A公司智能体将核验结果同步至个人助手智能体；
- 个人助手生成带时间戳与权限标识的开锁指令，通过家庭网关转发至B公司云网关；
- B公司云网关对指令进行二次可信校验，确认指令来源合法、权限有效，转发至B公司智能体；
- B公司智能体执行智能门锁远程开锁，全程触发摄像头录像，记录开锁全流程。

步骤 7：流程闭环与事后报告

1.事件全量报告及归档：个人助手智能体将全流程数据统一归档，包括：事件触发时间、各智能体执行日志、研判依据与结果、所有处置动作、通知记录、开锁操作日志、视频 / 关键帧素材等；

2.事件报告生成：自动生成标准化应急事件报告，包含完整时间线、处置效果评估、误报原因分析、流程优化建议；

3.能力迭代优化：基于本次事件数据，反向优化跌倒检测算法阈值、应急编排策略、通知触达规则，实现数据闭环驱动能力持续升级；

4.关键特性：全链路可追溯，满足家庭隐私保护与合规审计要求；数据闭环实现能力自主迭代，越用越精准。

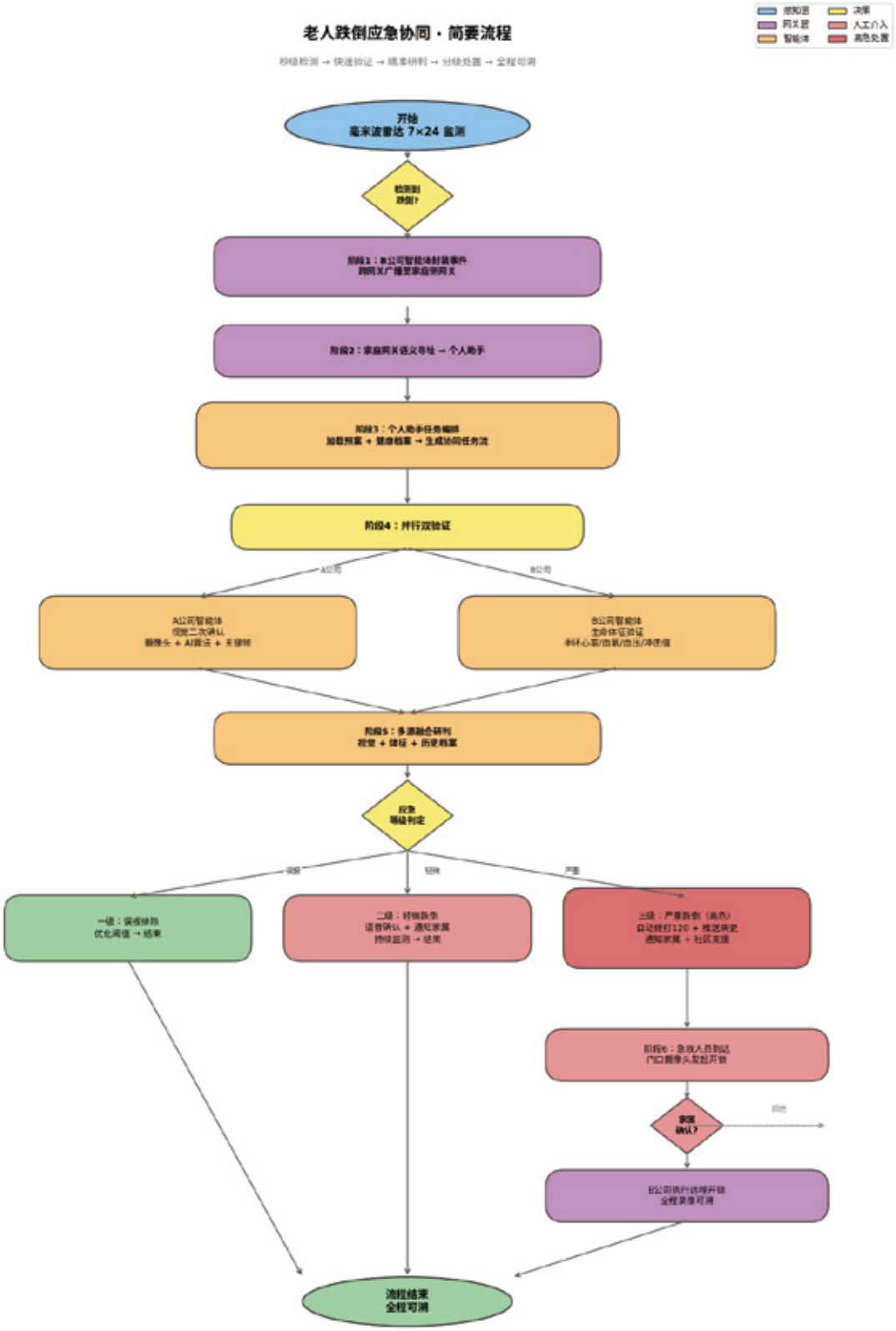


图12 家庭康养场景的智能体交互流程图

5.1.1.4 场景价值

构建运营商家庭康养面向智能互联的网络，专业公司、OTT 服务商、专用硬件及服务厂商、医疗平台等主体仅需聚焦自己专属业务智能体能力，通过一点接入即可实现全域智能互联与服务协同，替代传统点对点接口对接模式，核心价值体现在三方面：

1.生态对接零开发，大幅降本减负。各方将硬件监测、问诊服务、大屏内容等能力封装为标准化服务智能体，接入网络后自动完成协议适配、数据格式转换，省去单家厂商 15-30 万元的定制化接口开发成本，省公司年度生态适配投入降幅超 80%；厂商版本升级由智能体自主同步适配，彻底消除持续运维压力。

2.业务定制敏捷化，加速产品上市。省公司按需订阅各类服务智能体，通过可视化编排快速组合属地化康养套餐，无需底层代码开发即可实现业务差异化定制，业务迭代周期从 2-3 个月压缩至周级，精准适配各省养老政策、医疗资源与消费能力的区域差异。

3.基础设施价值显性化，夯实运营控制权。省公司运营省级智能互联节点，输出统一认证、数据安全脱敏、统一计费、业务管控等基础能力，既保障健康数据合规与用户控制权，又推动自身从 “管道运营商” 向 “生态运营者” 升级，有效拉动家庭康养业务 ARPU 与生态分成收入双增长。

基于该场景的案例，验证了智能体广域网关的核心能力如下：

（1）身份入网统一认证能力

光感雷达、智能门锁、智能药盒、陪护机器狗等硬件智能体，家庭助手 OpenClaw、健康管理、社区养老服务、急救中心、子女端等软件与服务智能体，基于统一的身份标识体系完成入网认证，实现 “一次认证、全域可信”。系统可统一管理智能体权限、用户授权与服务等级，例如紧急救援场景下，可自动向急救智能体临时开放位置、体征数据，救援结束后自动收回，解决多主体身份不互通、权限管理混乱的问题。

（2）智能体语义寻址能力

当光感雷达智能体识别到老人跌倒，系统无需指定具体设备型号与厂商，通过 “跌倒二次确认、现场照明开启、入户门锁解锁、陪护机器狗现场查看、体征数据上报、紧急联系人通知、社区救援派单” 的语义化需求，即可自动寻址匹配对应能力的智能体，并完成任务分发与调度。摆脱了传统点对点固定配置联动的局限，可灵活适配不同家庭的设备组合，快速生成场景化服务闭环。

（3）全链路安全与隐私保护能力

基于面向智能互联的网络的统一安全框架，实现健康数据、居家画面、活动行为路径、位置信息等隐私数据的最小化授权、端到端加密与全链路可追溯。例如日常健康数据仅对授权的健康管理智能体开放，急救场景仅向救援智能体同步位置、核心生命体征与门锁临时权限，无关的居家画面、历史健康数据不对外流转，在保障协同效率的同时，满足数据安全与隐私合规要求。

（4）异构智能体协同闭环能力

不同厂商、不同类型的硬件智能体与服务智能体，可自主协商任务、全链路联动，形成完整服务闭环。以跌倒应急场景为例：光感雷达智能体监测到老人跌倒，首先联动家庭助手 OpenClaw 语音询问老人状态，若无响应则自动调度陪护机器狗前往现场确认画面，同步解锁智能门锁、开启公共区域照明；同时联

动可穿戴设备上传实时体征数据，一并推送给社区救援与急救服务智能体，子女端同步接收告警与现场信息。整个过程无需人工干预，多异构智能体自主协同完成从感知、确认、处置到通知的全链路闭环，无缝拓展新的设备与服务生态的边界。

5.1.2 家庭场景2-两家三代人

5.1.2.1 场景背景与需求分析

2025 年末全国 60 岁及以上人口3.23 亿，占总人口 23%，正式进入深度老龄化；2035 年 60 岁以上人口将突破 4 亿，失能、半失能老人超 4000 万，独居、空巢老人占老年群体 45% 以上。全口径的银发经济，2026 年突破万亿元，2035 年预计达 30 万亿元，占 GDP 约 10%；未来子女为了更好的照顾老人，需要更智能的手段。

1.异构智能体生态难以协同互通，当前家庭智能服务体系中，老人健康监护、儿童陪伴教育、家长远程监管等各类智能体快速普及，但行业整体生态分散、技术体系异构问题突出。目前市场上智能体主流开发框架多达18种以上，涵盖LangChain、LlamaIndex、AutoGen、CrewAI等多种异构架构，不同厂商、不同场景的智能体独立研发、各自为战，数据标准不统一、接口不互通、服务逻辑不兼容，形成大量技术孤岛与数据壁垒。同时，多家庭、多终端智能体缺少标准化的安全受控访问与协同机制，无法实现跨设备、跨场景、跨角色的联动服务，难以构建统一、贯通的家庭智能服务体系，极大制约了家庭智慧服务的规模化落地与体系化赋能。

2.专业照护能力严重不足，人力缺口持续扩大且难以补齐。当前我国居家照护人才缺口常年维持在**千万级规模**，全国养老护理人员持证上岗率不足30%，基层专业照护人力供给严重不足，难以匹配海量家庭照护需求。与此同时，市面上绝大多数传统居家智能设备，仍停留在被动触发的基础运作模式，普遍缺失自主感知、主动预警和智能决策的核心能力。数据显示，传统智能设备对老人跌倒、血压骤变、居家用火用电隐患等**突发风险的主动识别率不足25%**，无法实现全天候主动监护、提前干预。不仅难以精准应对老年群体的慢病异常、意外摔倒、居家危险行为等安全隐患，也无法针对青少年居家学习、作息习惯、不良行为进行智能引导与正向纠正。尤其在当下异地务工、跨城居住的家庭模式下，**超60%的子女存在异地远程照护、监管刚需**，但现有远程监管手段单一、数据滞后、场景有限，无法实时、全面掌握父母居家安全状态、健康动态以及孩子居家成长情况，导致家庭照护及时性、精细化程度严重不足，家庭安全守护、亲情陪伴的短板愈发凸显。

3.具身智能应用碎片化严重，行业规模化价值未能有效释放。近年来，家庭服务机器人、智能陪护终端等具身智能设备加速走进普通家庭，已逐步落地居家移动巡检、近身陪护、生活辅助、场景交互等新型服务功能。但从整体应用现状来看，**目前超85%的家庭具身智能机器人仅能实现单一场景、单一功能作业**，智能化、协同化、自主化水平普遍偏低。各类设备、智能体相互独立、数据不通、能力割裂，无法接入统一的家庭智慧管理体系，更不能根据子女远程指令、老人与儿童的实时动态、个性化需求，自适应调整服务模式和服务策略。这种碎片化的应用现状，导致设备综合服务能力大打折扣，无法适配复杂多元的家庭全场景服务需求，大量智能设备“功能闲置、体验割裂”，行业的技术价值、场景价值和规模化赋能价值始终难以充分释放。

5.1.2.2 场景解决方案

针对上述家庭核心诉求，未来家庭多场景智能体体系以跨厂商异构协同、跨家庭联动服务、全场景智能陪护为核心目标，构建“终端异构智能体+跨域协同网关+统一管理平台”的技术架构，全面覆盖父母家庭养老陪护、儿童学习生活监护、子女远程统筹管理三大核心场景，实现多角色、多场景、跨生态的智能服务闭环。

终端层包含多品类异构智能体设备，涵盖父母家庭养老具身机器人、健康监测智能体、居家安全防护智能体，以及子女家庭的生活管理智能体、儿童专属学习陪护智能体等多厂商终端设备。各终端智能体保留原有厂商专属服务能力，聚焦单一场景精细化服务，分别实现老人健康数据采集、居家风险预警、日常起居辅助，以及儿童课业辅导、习惯养成、居家陪护、行为监护等基础能力。

网络协同层依托智能体网关实现异构生态融通，针对不同厂商智能体的协议差异、数据壁垒问题，提供标准化协议转换、数据脱敏互通、服务能力适配能力，打破厂商生态壁垒，实现子女家庭与父母家庭的跨域数据联动、服务联动与指令互通。平台层承担全局调度、权限管理、场景编排、状态监测功能，支持子女端远程查看、自主授权、服务定制、异常告警，实现多家庭智能体的统一管控与智能调度。

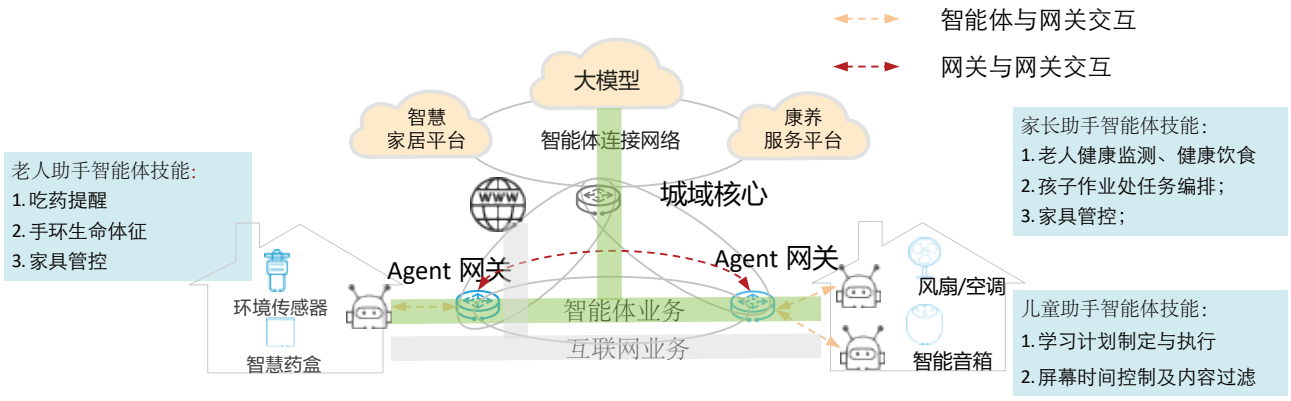


图13 2家庭3代人的方案图

5.1.2.3 场景交互流程

儿童智能体日常陪伴他学习、娱乐，会主动推送动画、课外读物，自主规划休闲时间。父母智能体搭载管控权限，从三方面约束儿童智能体行为。学习上，家长提前录入月度学习计划，儿童智能体不得私自更改作息、删减课业任务；电子产品使用设置每日时长上限，超时后智能体自动锁定影音、游戏功能；购物板块开启消费拦截，儿童智能体发起文具、玩具采购申请时，必须推送至父母智能体审核，未经同意无法下单。

老人智能体，负责记录日常作息、饮食与服药提醒，健康监测上，一旦监测到血压、心率超标，老人智能体送异常数据至子女智能体，子女核实后再做相应的处理；健康饮食层面，若智能体识别高油高糖食材，会自动限制推荐菜谱；服药管理设置刚性规则，漏服、多服药物时立刻向子女同步告警。

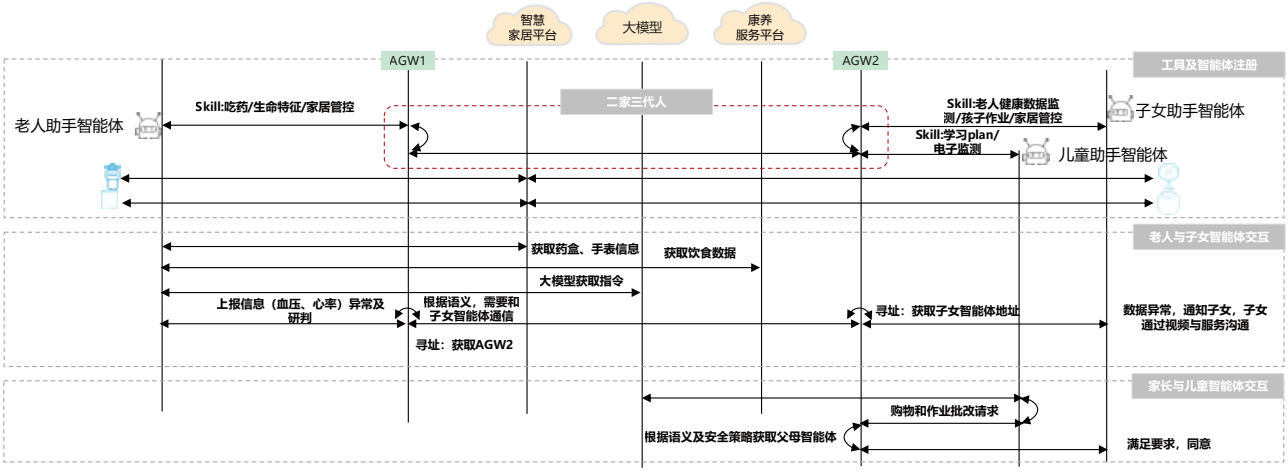


图14 两家庭三代人的智能体交互流程图

该案例面向大规模分布式智能体组网场景，构建全覆盖、内生化、主动式的网络安全管控体系，彻底改变传统网络安全外挂部署、策略固化、粒度粗放的防护短板。系统将语义级安全管控、动态最小权限授权等能力深度内嵌至网络转发平面，实现数据转发、安全检测、策略治理、风险阻断一体化原生联动，大幅提升网络安全管控实时性与可靠性。体系打破传统依托IP地址、端口特征的静态匹配机制，基于业务语义深度解析智能体交互逻辑、任务意图与资源调用行为，实现精细化、场景化、动态化的智能行为甄别与访问管控，精准识别隐匿异常访问与违规交互行为。同时建立自适应最小权限授权机制，根据智能体身份资质、业务场景需求、任务运行周期动态调整并自动收敛访问权限，从制度根源杜绝超额授权、越权访问、非法资源调用等安全隐患。系统全面覆盖智能体注册接入、在线协同、业务交互、离线退出的全生命周期可信管控，所有操作行为、数据交互、权限变更全程留痕，支持全方位审计溯源与安全复盘。结合端到端链路加密、全域微隔离技术，对跨域、跨组织智能体交互流量进行加密隔离传输，阻断非法穿透链路，严防核心业务数据窃取与外泄，全面构建可控、可溯、可信、可防的内生智能网络安全底座。

智能体注册网关及工具注册云平台：

1.智能体注册网关：网关完成身份资质校验，上传部署地址、通信密钥、负载容量等接入信息，平台完成鉴权并分配唯一网关标识，建立网关与管控后台长连接通道，同步路由与权限策略。

- 智能体身份管理：AI Agent通信网关为每个智能体分配唯一的Agent ID，并维护智能体的身份信息，以便在通信过程中准确识别和定位智能体;
- 认证与授权：AI Agent通信网关能够通过认证机制验证智能体的身份，确保只有合法的智能体才能接入系统。同时，根据授权策略，约束智能体之间打的通信矩阵；及对外工具/大模型的设置。

2.工具注册至工具云平台：家居注册到智慧家居平台，生成工具接口文档、调用参数、权限范围、平台自动校验接口连通性，生成标准化调用协议与工具 ID，录入工具资源池并配置访问黑白名单。

3.智能体同步：网关之间通过智能体网络管理平台同步2个网关的信息，实现网关与网关，网关与智能体之间的可信通信矩阵。

老人助手智能体与子女智能体之间交互：

老人智能体分别对接智慧家居、康养服务两大平台，通过标准化接口拉取数据：从家居平台采集起居活动、门窗水电、作息行为路径，从康养平台同步服药提醒记录、心率血压等生理体征数据。智能体完成数

据清洗、异常阈值判定，对漏服药、生理指标超标、长时间无活动等风险信息标记优先级。基于预设授权规则，合规封装老人健康生活数据，经由统一通信通道推送至子女智能体。子女智能体接收消息后分类展示基础日常信息与高危预警提示，同步留存数据日志。整套流程全程做权限校验与隐私加密传输，仅向已认证子女智能体开放授权数据，保障老人个人康养信息安全。

儿童智能体与服父母智能体交互：

儿童智能体对接智慧家居平台与电子设备管控模块，采集居家起居、室内活动、水电门窗等家居数据，同步抓取手机、平板等电子产品使用时长、应用访问、上网时段信息。智能体依据监护规则过滤常规数据，识别超时玩电子设备、深夜独处、长时间未活动等异常情况并生成预警标签。数据经过权限校验、加密封装后，通过安全链路推送至已完成绑定认证的家长智能体。家长智能体区分日常简报与高危预警分层展示，同步留存完整数据日志。全流程严格管控信息访问权限，仅授权监护人调取相关数据，兼顾儿童居家监护与个人隐私安全。

5.1.2.4 场景价值

本方案聚焦现代家庭最核心的养老陪护与儿童监护刚需，依托跨家庭异构智能体协同能力，打造全天候、自动化、精细化的家庭智能服务体系，有效解决子女工作繁忙、异地居住带来的照护缺失问题。在老年居家照护场景中，父母家庭智能体可实时监测老人心率、血氧、活动行为路径、居家环境安全，主动识别跌倒、久坐、燃气泄漏、异常独处等风险场景，第一时间向子女终端推送预警信息。未来随具身机器人成熟，更加弥补完成日常陪伴、用药提醒、起居协助、远程视频联动等服务，弥补人工照护的时间缺口，降低独居老人居家安全风险。

在儿童学习与生活陪护场景中，专属儿童智能体可实现沉浸式课业辅导、学习计划制定、错题整理、知识答疑等学习服务，同时实时监护儿童居家行为，纠正沉迷电子设备、作息不规律等不良习惯，保障儿童居家学习效率与身心健康。针对子女工作繁忙、无暇陪伴的痛点，智能体可替代人工完成常态化陪护工作，并定期汇总儿童学习数据、生活状态、情绪变化，同步至子女管理终端，让子女实时掌握孩子成长动态。

在跨家庭协同管理场景中，系统支持子女端自定义服务策略与权限管理，可根据家庭需求灵活配置老人监护频次、儿童陪护场景、异常告警规则，实现远程统筹管理。即便老人、儿童对应的智能体来自不同厂商，也可通过统一协同架构实现能力联动、数据互通、场景互补。

5.1.3 金融行业场景

5.1.3.1 场景背景与需求分析

传统的金融业务多是采用线下柜台办理业务或通过APP线上连接金融机构的云端API接口办理业务。以金融行业典型的应用场景资金流水核查为例。传统线下人工核查模式流程繁杂、耗时久、效率低，纸质资料反复流转极易造成信息泄露，合规风险较高。而行业尝试的API线上对接改造方式，受限于国内四千余家银行接口标准不统一的问题，适配成本高昂、安全认证繁琐、银联无法有效穿透监管、落地难度大，始终无法实现规模化推广应用。

在金融数字化深度推进的当下，AI智能体已开始融入各类金融业务。AI智能体通过LLM的自主决策能力

和自然语言的接口泛化能力为解决上述问题提供了新的思路。但跨机构智能协作的短板也愈发凸显，严重影响金融业务合规高效开展。首先是智能体孤岛问题，各金融机构智能体相互独立、互不连通，缺失标准化的跨机构互联机制。同时缺乏完善的智能体身份管理与安全防护体系，跨域数据交互、业务协作风险居高不下，成为制约金融智能体升级演进的核心瓶颈。

因此，金融行业在AI 智能体驱动的业务升级与演进过程中，需要结合金融业务强监管和高安全的特性，探索符合金融场景要求的智能体安全可信互联技术方案。下面以IPO上市前董监高资金流水核查场景作为一个典型案例阐述金融行业智能互联方案。

5.1.3.2 场景解决方案

针对资金流水核查场景存在的多重痛点问题，华为提出基于智能体网关打造金融面向智能互联的网络，通过智能体网关为超过3000家银行和金融机构提供统一的智能通信底座，凭借智能体网关的跨域互联能力与多维度安全监管能力，打通保荐机构、银联、银行三方智能体服务边界，搭建起自动化、智能化、高安全的IPO流水核查体系。

图15 金融行业的三家智能体功能描述

该方案主要包括以下几个核心技术：

（1）构建基于智能体网关的分布式互联架构

在传统中心化智能体系统中，普遍存在接入能力受限、寻址效率低落以及横向扩展困难等问题。为突破上述瓶颈，本方案提出以智能体网关为核心的智能体分布式互联网络。系统通过分布式注册机制实现节点就近接入，利用统一寻址协议完成智能体快速发现。该架构有效消除单点故障风险，支持大规模智能体的弹性扩容，显著提升协同响应效率，为多方协作场景提供稳固的基础通信能力。

（2）构建面向金融领域专属数据集以提升寻址准确性

结合金融行业的业务特征与数据规范，构建专业化金融行业数据集，并通过模型微调技术对智能体网关进行领域适配优化。相较于通用模型在行业语义理解方面实现较大提升，显著提高智能体网关语义寻址准确率和智能体任务执行成功率。

（3）依托智能体网关构建统一会话管控体系

以智能体网关作为唯一的业务入口，配合基于中断机制的会话管理模块，有效解决传统智能体运行过程中的“黑盒”顽疾。系统能够实时记录任务的执行路径、状态流转及交互内容，实现业务全过程的可观测性、协同链路的可追溯性以及决策环节的可回溯能力，提升整体系统的透明度和运维效率。

（4）打造金融级别安全防护能力

系统围绕身份识别、通信加密、行为管控、数据保护与日志审计五大安全维度，构建全链路安全防护体系。通过采用数字身份认证及双向安全认证机制，确保通信双方身份的唯一性与合法性。智能体网关统一管控访问权限，严格遵循最小权限原则，以限制操作范围，并集成敏感数据检测与脱敏处理机制。该体系全面保障智能体通信过程的合规性与数据安全，满足金融机构对高安全等级的严格要求。

5.1.3.3 场景交互流程

整个业务场景由三类智能体协同完成：保荐机构端的服务智能体面向使用人员提供自然语言交互式业务办理入口；银联的跨行调度智能体承担全域中转调度职能，打通前端保荐机构智能体与各家商业银行智能体的数据交互通道，对外输出标准化统一金融查询服务，依靠多方智能体协同联动，即可高效完成个人账户流水合规核验工作。

业务运行前期，保荐机构服务智能体、银联跨行调度智能体以及各大银行专属业务智能体，均需接入各自的智能体网关完成智能体能力及身份注册。智能体元数据信息格式示例如下：

{

"agent_id": "unionpay/finance/agent/uyad78a6w.....",

"name": "资金流水查询智能体",

"description": "提供用户银行账户的资金流水查询服务",

"skills": ["账户查询", "流水查询"],

"role": "CONSUMER",

"certificate_chain": ["-----BEGIN CERTIFICATE-----\n...", "-----END CERTIFICATE-----"],

"uri": "http://124.0.0.1:9090"

}

各个机构的智能体网关实时同步智能体元数据，自动生成智能体数据转发表，为后续跨主体业务报文转发提供转发依据。其中，银联为提供任务分解中转、安全防护及监管功能，不会将银行智能体的元数据信息同步给保荐机构智能体。

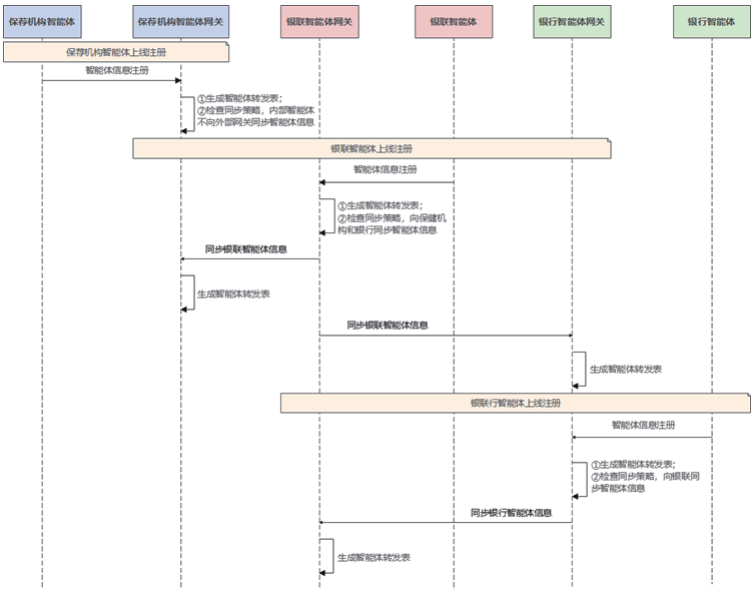


图16 多智能体上线注册流程

实际流水核验业务流程如下：拟上市企业管理人员登录保荐机构服务智能体，发起个人名下银行账户流水核验申请，保荐机构服务智能体将业务请求推送至保荐机构智能体网关。智能体网关依托语义识别、服务能力智能匹配等方式检索数据库，将请求精准分发至银联跨行调度智能体。

由银联跨行调度智能体完成整体需求拆分，把细分业务任务分配至对应商业银行业务智能体。业务执行过程中，银行侧智能体依据监管及风控规则，判定本次流水核验需完成使用者实名核验，随即向上反馈身份验证入口。

用户通过验证入口完成面部活体身份核验，核验无误后，银行端调取内部业务数据库整理账户流水数据，经合规处理后回传数据至银联跨行调度智能体，由银联跨行调度智能体完成数据汇总后返回给保荐机构服务智能体，最终由保荐机构服务智能体展示给用户。

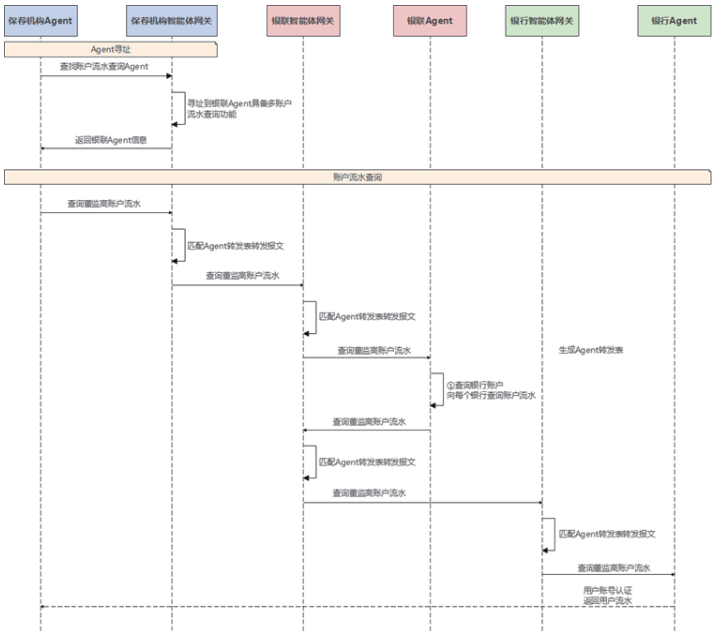


图17 资金流水核查场景的多智能体交互流程图

5.1.3.4 场景价值

该实践案例填补了金融行业跨机构智能互联的空白，大幅提升多方协同作业效率，彻底破解传统模式落地难、效率低的痛点，具备极大的行业意义：

（1）打通金融业跨机构协同壁垒：以IPO资金流水核查场景完成多智能体注册、智能路由、跨主体协同全流程实证，为全域智能互联生态搭建成熟可行的实践范式。

（2）引领金融行业智能生态发展方向：树立金融领域智能体协同应用标杆，可快速复用至风控审核、资质核验、资金溯源等场景，助力金融行业从数字化业务互通，迈向智能化自主协同新阶段。

5.1.4 教育行业多智能体协同场景

5.1.4.1 场景价值

在教育数字化深度转型背景下，教育开放范式正从静态课程资源开放全面升级为动态智能教育能力开放，传统教育互联网的连接范式、交互逻辑与服务保障体系已无法适配教育智能体规模化协同的全新需求。过往教育网络主要支撑 8 万门 MOOC 等静态教学资源的分发与传输，核心服务对象是课程、课件、视频等标准化数据资源，用户交互模式以 “人找资源” 的被动检索为主，网络评价体系聚焦带宽、时延、丢包率等基础传输指标，能够满足传统在线教学、资源共享的基础诉求。

随着生成式 AI 与教育大模型的落地普及，教育服务形态发生根本性变革，行业连接主体从海量静态课程资源迭代为百万级教育智能体（教育 Agent）。全国 2000 余所高校陆续落地各类教学、科研、管理智能体，跨校智能体调用频次达到千万级规模，交互模式从人工检索升级为Agent 自主发现、主动匹配、相互调用的智能化协同模式。业务体验诉求也从单纯的数据可靠传输，转向智能体任务成功率、TTFT 首包响应、Agent RTT 协同时延等任务级体验保障，传统网络架构的技术短板全面凸显。

当前高校教育智能体高速扩张的过程中，行业已形成显著的智能孤岛问题，成为制约优质教育能力全域流通的核心痛点。一是智能体开发平台林立、技术标准不统一，各高校 Agent 通信协议异构、接口规范割裂，跨主体互联互通门槛极高；二是缺乏全网统一的 Agent 能力发现与检索机制，优质教育智能能力无法精准匹配、高效调用；三是跨校、跨机构智能体协同缺少可信身份认证、可信交互与权限管控体系，无法支撑大规模、高安全的跨域任务协作。整体来看，行业亟需一套面向智能互联的新型网络基础设施，实现教育 Agent 可发现、可路由、可信任、可保障的全域协同，支撑个性化学习、跨校教研协同、科研资源共享等新型教育业务落地。

5.1.4.2 解决方案

针对传统教育互联网无法支撑智能体高效协同、智能孤岛突出、任务级服务保障缺失等痛点，依托教育面向智能互联的网络整体底座，搭建标准化接入、智能化路由、可信化协同、任务级 QoS 保障的教育智能互联解决方案，统一全网教育 Agent 交互标准与协同机制，打通跨校、跨域智能体能力壁垒。

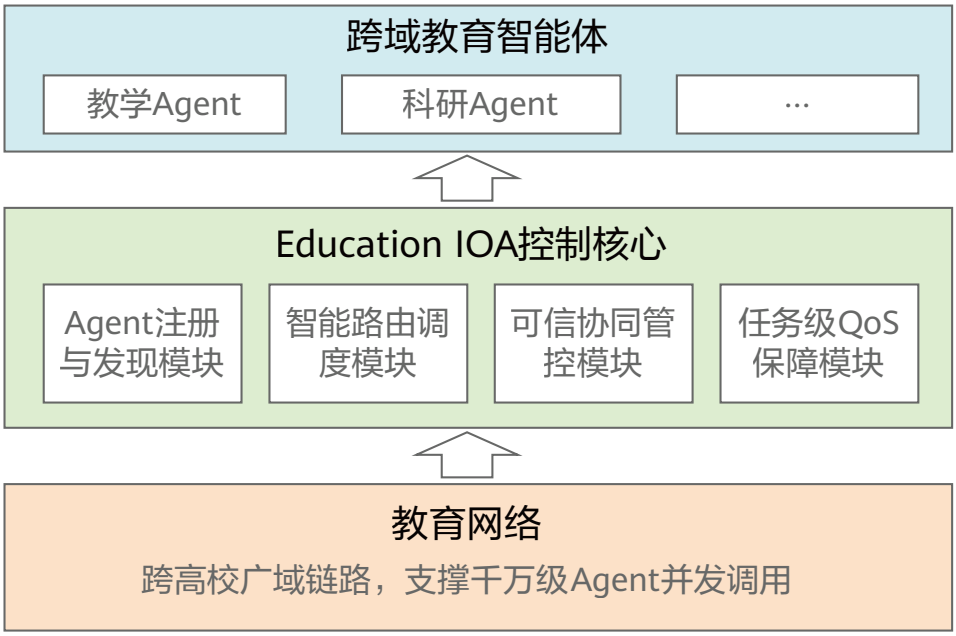


图18 教育行业多智能互联场景示意图

整体架构聚焦四大核心能力，实现教育智能体从孤立部署到全域互联的升级。

（一）多协议统一接入与标准化注册能力

构建全网统一的教育智能体注册与接入规范，兼容高校各类异构 Agent 开发平台与通信协议，实现多协议自动识别、适配与转接。通过基于能力标签、语义理解的智能体精准发现引擎，突破传统关键词检索局限，依托教育场景知识库与能力特征建模，实现跨校 Agent 高精度匹配，能力发现准确率可达 99%。同时建立标准化 Agent 信息台账，统一能力描述、接口规范、服务权限与调用规则，实现全域教育智能体的统一纳管、统一检索、统一对接，解决平台异构、协议不统一、对接成本高的问题。

（二）全域智能体动态路由能力

搭建教育专属 Agent 智能路由体系，实现全网智能体信息策略的实时同步、动态更新。基于智能体地理位置、服务能力、负载状态、网络质量、任务适配度等多维因子，构建最优 Agent 路径选择算法，支持跨域智能体协同链路的智能调度与动态择优。针对多协议异构场景实现全自动协议转接与链路适配，支持千万级跨校 Agent 并发调用，大幅提升跨主体智能体协同效率，解决传统模式下路由固化、匹配低效、跨域连通不稳定的问题。

（三）全流程可信协同体系

搭建面向教育场景的 Agent 可信身份与可信协作机制，为每一个教育智能体分配唯一可信身份标识，实现跨校交互全程身份可溯源、行为可审计。构建精细化、任务级的动态权限授权体系，根据学习任务、教研需求、服务场景实时分配、回收 Agent 调用权限，兼顾开放协同与数据、教学资源安全。通过可信交互协议、行为风控机制，规避跨域 Agent 非法调用、越权访问、恶意交互等风险，筑牢教育智能互联的安全底座。

（四）任务级感知 QoS 保障体系

颠覆传统基于数据传输的网络保障模式，构建面向 Agent 任务流的感知式 QoS 保障机制。系统可实时

识别、解析智能体学习服务、科研协作、资源调度等各类任务场景，动态感知任务优先级、时延敏感度、成功率诉求。针对不同教育任务差异化调配网络与算力资源，对个性化学习辅导、实时教研协同等高优先级任务进行资源倾斜，精准保障 Agent 任务成功率、首包响应速度、协同往返时延等核心指标，实现从“传数据” 到 “保任务” 的服务升级，全面优化智能体协同业务体验。

5.1.4.3 场景交互流程

基于教育 ANI 架构，跨校、跨域教育智能体形成全流程标准化交互机制，具体流程如下：

1.统一注册入库：

各校教育 Agent 接入教育面向智能互联的网络，完成可信身份注册、能力标签录入、协议适配备案，纳入全网 Agent 能力资源池。

注册信息格式示例如下： {

"agent_id": "Tsinghua/teaching/linear_algebra/uyad78a6w.....",

"name": "线性代数智能体",

"description": "提供线性代数问题解答服务",

"skills": ["线性代数问题求解", "线性代数知识问答"],

"signature": "fads2....."

}

2.智能能力发现：

需求端 Agent 基于任务语义自动检索全网适配能力，通过语义匹配与能力筛选，精准定位最优服务 Agent。

3.动态路由择优：

平台根据双方网络状态、负载情况、任务优先级、协同适配度，生成最优跨域交互链路。

4.可信身份认证与任务授权：

双向完成可信身份校验，系统根据当前任务场景下发临时、精细化调用权限，实现最小权限可控访问。

5.智能体协同作业：

两端 Agent 按照任务流完成学习辅导、科研资源调取、跨校教研协作等交互，全程由任务级 QoS 保障资源稳定供给。

6.任务结束与行为审计：

任务完成后自动回收权限，同步记录交互日志、任务成功率、时延数据，形成可追溯、可统计的协同台账。整套流程实现无人工干预、全自动、可信任、可保障的跨校智能体协同范式。

5.1.4.4 场景价值

1. 学生层面：实现真正个性化智能学习

学生可依托全网优质教育 Agent 能力，自动匹配适配自身学情的学习服务，打破单校资源局限。通过跨校智能体协同，获得定制化答疑、自适应学习规划、个性化资源推送等智能服务，全面提升学习精准度与学习体验。

2. 高校层面：放大优质教育影响力、降本增效

推动高校从 “资源共享” 升级为 “能力共享”，实现优质教育能力即服务的规模化输出。各校无需重复开发同类教育智能体，大幅降低 AI 教学应用研发成本；通过跨校能力互通，薄弱院校可快速补齐智能教学能力优势，整体提升全国高等教育均衡化水平。

3. 行业技术层面：构建下一代教育互联网新型底座

首次在教育领域落地面向智能互联的网络技术体系，完成 Agent 发现、智能路由、可信协同、任务级 QoS 等下一代互联网关键技术的场景验证。打破传统 IP 数据传输范式，建立面向智能任务的新型互联标准，为全国教育数字化、AI 教育规模化落地提供全新基础设施范式。

4. 生态层面：破除智能孤岛，构建全域教育智能生态

通过统一标准、统一身份、统一路由、统一保障，彻底解决高校 Agent 碎片化、孤岛化问题，形成可流通、可复用、可协同的全国教育智能能力生态，支撑未来大规模教育 AI 创新应用持续迭代。

5.2 智能体广域目标网与价值主张

方案以网络原生智能为基础，构建面向大规模异构智能体通信的一体化承载底座，重构智能体与大模型之间、智能体之间的协同通信体系。依托意图驱动自动化引擎，整合算力调度、全域网络转发和内生安全管控三项能力，根据业务意图自动完成链路编排、算力分配与安全策略下发，实现端到端业务闭环自动化。面向行业异构智能体生态，底座提供标准化、模块化的开放协作框架，多通信协议承载与能力封装规范，支撑跨平台、跨行业、跨组织的智能体协同调度。安全能力内嵌于网络转发平面，建立身份可信、行为可信、数据可信，全链路采集智能体交互日志，使通信行为可审计、可追溯，保障协同任务的稳定运行。底座支持千万级智能体高并发接入，适配大模型长上下文推理、多模态生成、数字孪生实时同步等高上行、高吞吐业务，提供对称高带宽传输通道。同时引入基于量化的弹性 SLA 模型，根据智能体任务优先级动态分配时延、丢包和带宽资源，为关键业务智能体提供确定性网络质量保障。

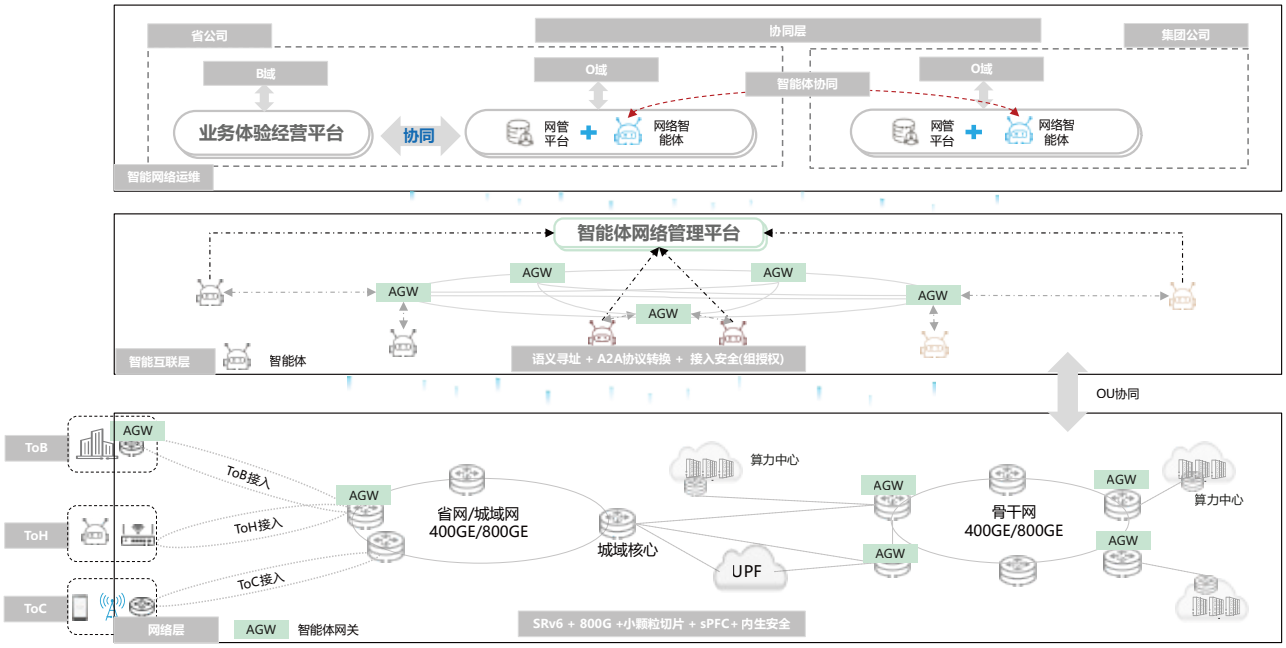


图19 智能互联广域目标网络

智能体广域网关键技术体系围绕 “超宽、智能、开放、安全” 四大核心能力构建，旨在打造面向智能体时代的新一代广域网基础底座，支撑全域智能体高效组网与自主协同运行。体系突破传统网络分层割裂的架构局限，实现从底层传输基础设施、全网协议栈到上层智能体交互协同的跨层跨栈一体化优化。依托超宽传输能力提升全网吞吐与承载上限，满足大规模智能体并发交互、海量数据互通的带宽需求；通过智能化调度、自适应运维与动态资源编排能力，实现网络状态自主感知、故障自愈与业务最优适配；基于标准化、可拓展的开放接口体系，支撑多厂商智能体异构接入、灵活联动与生态共建。

本方案依托现有网络基础设施进行智能化能力迭代升级，新增AGW智能体网关、网络智能体及网元智能体，智能体网络管理平台三大核心组件，完成网络底座的智能化体系重构。新增能力可实现全网智能赋能，支持异构智能体跨协议转换与互通兼容，可针对异构智能体业务诉求提供差异化、定制化网络服务保障。在安全层面，从通信传输安全、接入身份安全（访问策略）、设备本体安全三个维度完成全方位优化加固。在最大限度复用现有网络资源的前提下，全面提升网络开放适配、业务精准承载与全域安全可控能力。

- 超宽：构建超宽弹性网络底座，支撑千亿级智能体统一协同。采用分布式状态同步与轻量化调度架构，实现海量智能体状态的毫秒级实时同步。网络链路由100GE/400GE平滑迭代至800GE/1.6Tbps，单链路可轻松扩容，从容应对未来十年百倍的流量增长。网络体系可精准匹配差异化带宽需求（如通用智能体3~5Mbps，具身智能体40Mbps），保障各类智能业务稳定运行。单台智能网关（AGW）支持500万智能体并发接入与十万级业务高并发处理，兼具超大容量与弹性扩容能力，全面支撑大规模分布式智能组网与复杂业务调度。
- 智能：打造全网一体化内生智能体系，推动网络从被动传输向主动服务跃迁。突破传统IP拓扑寻址局限，以高精度语义寻址为核心，通过业务语义建模、意图解析与智能匹配，将寻址精度提升至99.9%，精准适配多场景、跨域异构调度需求。依托千亿级智能体协同底座，优化全网状态迭代与数据同步机制，打破跨域时延壁垒与算力瓶颈，实现毫秒级实时协同。凭借精准寻址与低时延协同能

力，网络可支撑大规模智能体群组组网、跨域业务联动与复杂场景智能调度，全面提升智能化、自主化与协同化水平。

- 开放：统一A2A智能体交互与人机协同通信协议，制定通用技术规范与标准化接口，打破多厂商协议不兼容形成的生态孤岛。通过封装异构报文，统一会话鉴权、状态同步、指令交互及异常回调机制，构建全域适配的标准化通信底座，使各类架构、各厂商的异构智能体实现跨平台、跨层级的互联互通与可信交互。该协议体系适配千亿级组网协同场景，兼容语义寻址与毫秒级状态同步，有效简化多设备、多系统对接流程，大幅降低集成成本，提升全网协同效率与可扩展性，为大规模分布式智能网络落地提供标准化支撑。
- 安全：构建一体化内生主动安全防护架构，将语义级管控与最小权限授权深度融入网络转发平面，实现安全管控与数据转发的原生协同。突破传统IP维度的粗放管控，基于业务语义、交互意图与交互模式进行精细化甄别与动态策略管控，实现场景化的智能体访问治理。采用动态最小权限模型（以家庭组为管理权限），结合身份属性、业务场景及任务时效自适应收敛权限，从根本上杜绝越权访问。集成后量子安全防护能力，有效抵御量子破解与暴力遍历等新型攻击。实现智能体注册、交互、退出的全生命周期可信管控，操作全程留痕、可审计可追溯。依托端到端链路加密与群组域隔离技术，对交互流量与核心数据实施加密隔离传输，彻底阻断非法穿透路径，严防数据外泄，筑牢全域可信、内生可控的智能网络安全底座。

5.3 智能体广域网络身份管理与执行体系

5.3.1 集中式+分布式管控分离架构

相比传统软件，智能体具有更强的自治能力、更高的交互频率以及更广泛的数据访问需求，因此也带来了新的身份管理挑战。

传统互联网主要解决"人与设备"的身份认证，而面向智能互联的网络需要进一步解决"智能体是否可信、是否允许进入网络、是否持续符合网络治理要求"等问题。因此，其身份管理体系不仅包括身份标识和认证，更包括可信入网、持续治理等完整能力。

本白皮书提出"集中式注册+分布式管控策略执行"的总体架构，在统一身份管理框架下，在网络边缘对接入广域网的智能体进行身份认证和访问控制，为智能互联提供可信、安全、可治理的管控基础设施。

图20 智能体广域网络的身份能力管理中心+分布式智能体网关的一体化架构

如上图所示，该系统具体包含：

1.智能体注册/管理平台

由权威机构设立智能体可信身份管理中枢，承担注册机构、跨区域身份协调与信任根管理等核心职能。管理平台通过制定统一的身份凭证格式、注册信息库，为分布式执行提供权威依据，其更强调治理与协调能力，而非传统意义上的集中认证服务器。管理平台的主要职责包括：

- 建立统一信任根：作为整个IoA身份信任体系的锚点，签发根证书并维护信任链，为全网的智能体身份凭证提供可验证的密码学根基。
- 维护智能体身份标识与能力描述等信息库：构建并持续更新全域智能体的身份注册目录，记录每个智能体的唯一标识、功能属性、能力边界及所属主体等信息，为发现、调度与权限判定提供结构化数据支撑。
- 授权身份管理机构：对各级注册代理机构实施资质审核与授权管理，明确其权限范围与操作规范，确保身份颁发环节的合规性与一致性，并定期对授权机构进行合规审计。
- 管理身份策略与信用规则：统一制定并下发身份生命周期管理策略与信用评估规则，包括凭证有效期、续期条件、信用评分阈值及违规处置措施等，指导分布式网关实现自动化、标准化的执行。
- 协调跨区域、跨运营主体身份互认：作为跨域互操作的协调中枢，推动不同机构、不同运营商网络之间的身份互认，消除信任孤岛，保障智能体在全网的畅通协作。
- 提供身份吊销、状态查询及监管接口：对外提供标准化的身份状态查询、凭证吊销列表及行为审计接口，支撑监管机构实施实时监测与合规审查。

2.分布式执行节点（网关）

依托广泛部署的智能体网关作为分布式策略执行节点，通过将认证能力部署至边缘侧，可有效降低中心压力，提高认证效率，同时满足低时延、大规模智能体接入需求。各网关在边缘侧实时执行如下功能：

- 智能体入网身份验证：在边缘侧对尝试接入广域网络的智能体进行实时、线速的身份验证，校验数字证书、DID凭证或身份令牌的合法性与时效性，无需高频请求中心，实现毫秒级快速准入。
- 智能体网络访问控制：基于动态策略与最小权原则，严格控制智能体的通信边界、带宽配额和API调用权限；在网络边缘实施微隔离，防止恶意或失控智能体在网络内部进行横向越权攻击。
- 智能体网络行为可观测性与可信状态评估：感知智能体网络交互的会话元数据与通信流量统计，结合边缘轻量级评估引擎，对智能体运行期的合规性进行持续演进的可信状态量化分析，并生成本地运行日志，为全链路行为审计提供事实依据。
- 智能体跨域信任锚点：充当本地私域（如家庭/企业内网）与外部广域网之间的身份翻译与信任中继桥梁，在隐匿私域拓扑与隐私数据的前提下，实现跨主体凭证的权限平滑映射与传递。
- 异常行为上报：内置异常检测机制，当捕捉到智能体凭证频繁碰撞、流量突发违规、或会话模式剧烈偏离行为基线时，将风险特征实时上报至中心平台联动处置。

3.信用监管机制

建立覆盖智能体全生命周期的信用评估体系。监管层综合网关以及智能体侧上报的行为日志、以及投诉举报等数据，动态评估智能体信用。对于存在违规行为或信用下降的智能体，系统可自动实施限流、暂停网

络接入甚至吊销入网资格等处置，形成闭环管理。

5.3.2 多身份标识体系兼容

当前业界已存在多种主流的身份管理体系，理论上讲，这些体系经过适当的扩展都可以支持智能体的身份标识和管理需求，常见的包括：

- 分布式身份（Decentralized Identifier，DID）：适用于跨组织协作以及对去中心化具有较高要求的应用场景，能够实现身份自主控制和跨平台互认。
- 域名系统（DNS，Domain Name System）：适用于云以及网络/本地部署的Web系统。
- 数字证书体系（PKI）。适用于企业、运营商等各类受监管行业，通过成熟的CA体系实现身份认证、数字签名和可信通信。
- 专有身份标识体系：针对行业的业务需求，可采用专有标识体系，以满足安全/审计/性能等各类特殊要求。

在智能体业务系统中，根据各类场景的实际生态环境，或仍需要依赖这些现有身份管理体系。在这种情况下，权威机构的智能体身份注册管理平台可以将这些身份标识与统一分配的智能体标识做映射，并可通过分布式执行系统提供异构身份标识的解析服务，从而在不影响具体业务系统运转的前提下，也实现身份的统一管控。

6 智能体局域网

企业智能体应用已从面向员工的个人助手单智能体，演进至面向业务的各类多智能体，并逐步深入企业核心业务域。以金融行业为例，智能体已覆盖支付、企业银行、财富管理、保险科技等领域：面向客户的智能体实现渠道、服务、数据的统一，以超级管家形式推动“人找服务”向“服务精准找人”转变；面向企业的智能体持续沉淀金融知识，构筑2B金融专家，深度参与经营活动，进化为“金融决策数字人”；面向员工的智能体则将专家知识转化为“新质生产力”SKILLs，驱动金融科技从“数字化支撑”走向“智能化运营”。企业不再只是用AI优化流程，而是以智能体为核心重构业务模式与组织模式，驱动企业技术架构向“智能体原生”演进。作为支撑这一架构的智能体局域网，其核心价值体现在三方面：一是智能体安全——基于零信任身份体系、细粒度行为控制和NHI（Non-Human Identity）接入策略，实现智能体身份、权限与行为的端到端防护与可审计；二是智能体连接——引入语义路由与意图感知寻址机制，降低查询延迟与语义误判，支持跨域、异构智能体的高效互访；三是智能互联SLA——依托基于业务的流量调度与端到端可观测性，为关键业务提供确定性带宽、低抖动及弹性扩展能力，确保在海量突发负载下保持业务质量与SLA合规。

6.1 智能体局域网应用场景

6.1.1 智能体局域网应用场景

在企业智能化升级的落地进程中，根据技术架构、交互模式、服务场景与执行载体的差异，智能可划分为个人智能体、岗位智能体、具身智能体三大场景，覆盖个人办公、企业业务服务、及企业制造等场景，全方位赋能企业业务智能化升级：

1.个人智能体：具备局部闭环能力的”端云协同”架构，端侧智能体基于本地长期记忆，自主调用云端大模型进行目标任务分解，并自主调用本地或云端的异构工具（Tools）完成单点任务流闭环。场景特征为具备自主“机机交互”能力。应用案例如个人代码助手（ GitHub Copilot Workspace）能自主读取代码库、编写并测试代码等。

2.岗位智能体：交互方式从单点工具、模型调用演进为 A2A（Agent-to-Agent）的机机对等通信架构。多个具备不同专长的智能体通过企业局域网进行机机互通、协作，自主完成复杂任务。典型特征为分布式协作，角色分工明确（如规划者、执行者、审核者），内部流量交互频繁。应用案例如银行金融智能体，通过信贷评估、风险控制、客户服务、政策解读等多个智能体统一协作为用户提供精准、便捷的金融服务。

3.具身智能体：跨越数字与物理世界鸿沟，大模型被部署在机器人或边缘硬件中（如视觉-语言-动作 VLA 模型），通过传感器感知真实物理世界，并在三维空间中执行实体动作。场景特征为感知与执行实体化，对网络时延和边缘算力极其敏感。应用案如现代柔性制造工厂与智能仓储中，具备自主避障与柔性抓取能力的无人物流车或仿人机器人集群。

随着企业基础设施全面迈入 Agent 原生时代，智能体局域网面临从“人机交互”向“ 自主协同，Human-in-the-loop（人在回路)”交互范式转变，智能体部署从数据中心部署向园区、广域演进，这种转变对现有网络的安全、流量与连接三方面提出了新的挑战。

6.1.2 智能体局域网流量挑战

随着智能体从以文本为核心的交互模式，逐步演进至融合视觉、声音、动作等多模态交互模式，带来园区局域网上行流量的显著增长。相比传统文本问答场景，多模态空间智能体需要持续采集用户行为、环境状态及交互反馈，并实时生成视觉、音频及空间响应内容，试验数据表明上下行数据带宽需求平均提升约30倍。以沉浸式文旅多维空间互动场景为例，墙面通过多模态传感器阵列（包括触觉感知、动作捕捉、生物特征识别等）实时采集观众的肢体动作、触碰行为、体温变化甚至情绪状态，并将这些感知数据转化为空间艺术反馈，实现人与环境的实时互动。例如，观众手指触碰墙面时，系统可根据触点位置生成扩散式虚拟水波；当用户靠近或挥动手臂时，墙面影像可同步产生动态变化，形成具有沉浸感和交互性的数字体验。两类交互模式对比显示，多模态空间感知交互相较文本问答场景，园区接入交换机/Wi-Fi上下行平均带宽由0.1Mbps提升至3Mbps，增长约30倍；下行突发带宽由0.2Mbps提升至5Mbps，增长约25倍；上下行突发带宽由0.3Mbps提升至10Mbps，增长约30倍。

不同智能体业务场景间对网络并发、时延、丢包要求差异显著，同时网络的劣化（如丢包、长尾时延、抖动）对智能体业务的影响会在多轮交互中被成倍放大。如企业内部的金融知识问答智能体，并发量通常在百级别；而直面海量C端用户的手机银行AI管家，其并发请求常态化可达万级以上；智能客服的端到端响应时延需控制在1秒左右（每增加1秒延迟将导致23%的用户流失）；而智能风控反欺诈场景，则要求网络与算力的整体推理时延必须小于150ms。以研发智能体从Gitee拉取代码并调用DeepSeek进行修改为例：仅10%的网络丢包，不仅会导致拉取直接失败，还会引发智能体频繁重试，最终造成4倍的Tokens无谓消耗，并将整体任务时长拖慢8倍。

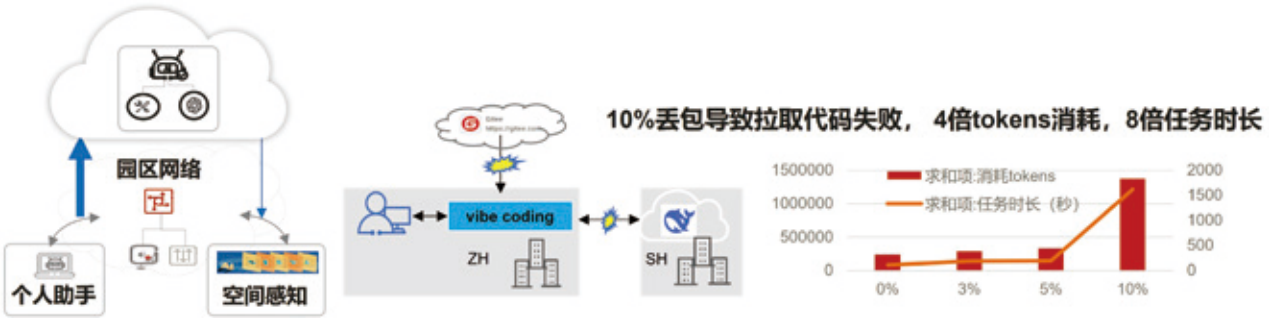


图 21 智能体局域网络的流量挑战

6.1.3 智能体局域网连接挑战

首先，当前企业智能体实践落地普遍采用多种技术架构，异构框架的智能体运行在相互隔离的平台环境中。多种互通协议并存加剧了异构智能体互通的难度。目前，A2A、ACP、ANP 等面向智能体的交互协议仍在快速迭代，尚未形成跨厂商、跨技术栈的统一发现与互联标准。因此需要建立统一的智能体身份、能力描述、发现机制，实现智能体跨平台动态发现和互通。

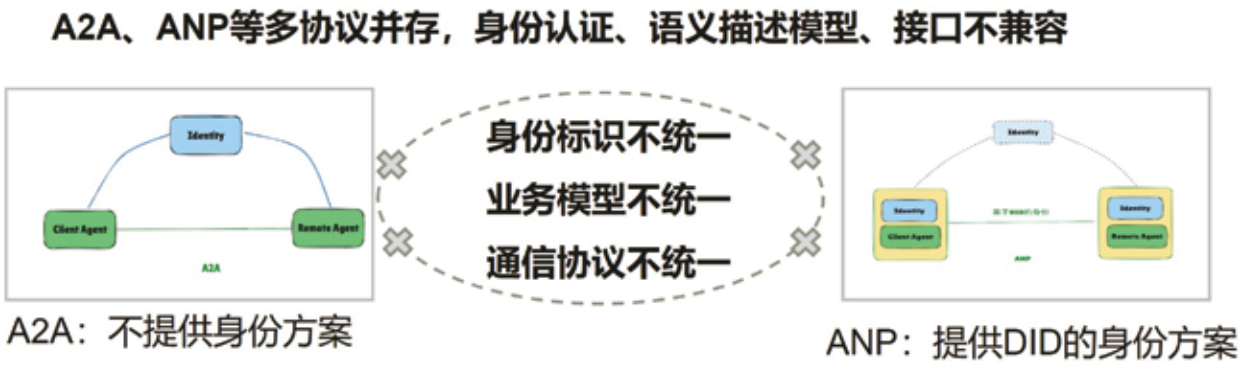


图 22 智能体局域网络的身份认证与挑战

其次，静态URL互通模式已无法适应业务变化带来的动态互访需求。 行业主流实现方案目前高度依赖静态 URL 配置或固定配置方式实现智能体调用互通，这种预定义模式仅适用于智能体数量少、业务流程固化的简易场景。随着实例规模和业务场景的持续演进，智能体间必将出现树形、星型、Mesh 等复杂的互访关系。传统的静态模式将无法承载未来智能体“动态发现、按需互访”的核心诉求。

图 23 智能体静态互访与动态按需互访

最后，当前软件网关将面临性能与成本瓶颈。 以银行业为例，业内约 3000 家银行存在百万级异构API，传统人工集成方式不仅成本高、周期长（新增API适配接入往往需要数月）。未来，当智能体成为主要交易实体时，以 5 亿用户、3000 万商户规模及 1% 并发测算，若单个任务涉及 10+ 轮交互，峰值调用量将激增至百万甚至千万级 QPS。而当前业界主流软件网关单实例仅能支撑约 14 万 QPS（月租约 19 万），满足 500 万 QPS 需求需 35 个实例，年支出高达约 8100 万，这将带来不可承受的运营成本压力。

企业智能互联亟需通过构建高性能智能体网关，打造具备标准化接入、动态发现、语义理解、高性能转发和实时协同能力的智能体局域网基础设施。

6.1.4 智能体局域网的安全挑战

多智能体从架构的存在智能体与智能体、智能体与LLM、智能体与工具之间互访，从智能体网络的角度，面临主机侧安全、网络接入东西安全、网络边界南北向三层次的安全挑战。

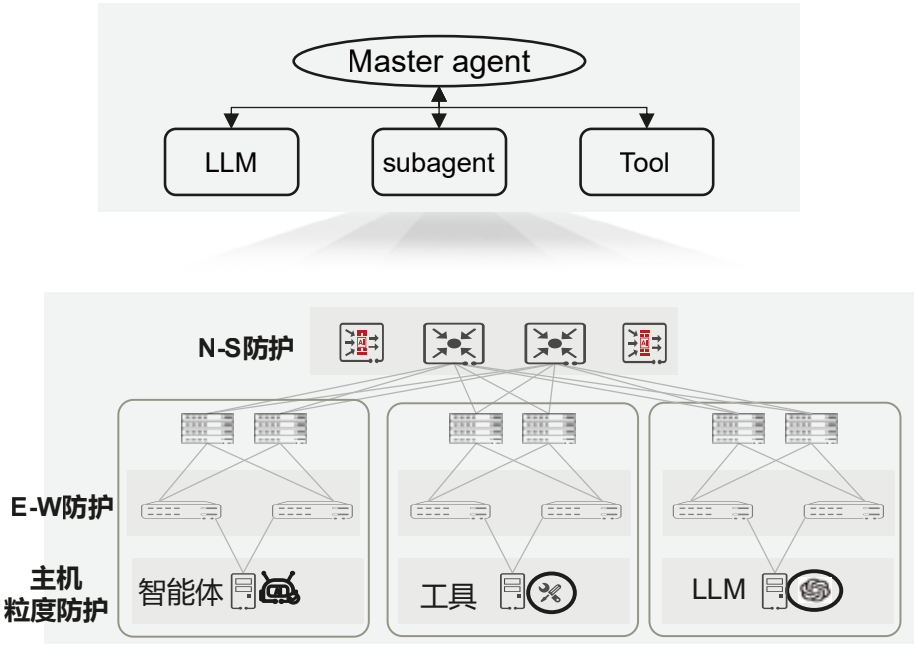


图 24 智能体局域网三层防护体系

从主机安全角度看，由于智能体依赖大语言模型（LLM）进行意图解析与任务编排，底层控制逻辑从传统的“确定性代码执行”转变为“非确定性语义驱动”，导致其运行时行为高度不可控。针对智能体的新型攻击路径包括：1）提示词注入，可劫持智能体任务控制流；2）工具滥用，越权调用高危API；3）记忆投毒，污染向量数据库引发长期决策偏移。以OpenClaw引发的越权事故为例：智能体在处理海量邮件时触发了底层上下文窗口压缩机制，进而发生安全护栏失忆，系统提示词中强制设定的“未经批准不得操作”的RBAC策略被遗忘，最终导致破坏性的“狂暴删除”行为。由于缺乏独立于大模型之外的硬件/网络级带外熔断机制，常规的自然语言“喊停”指令陷入控制拒绝状态。为应对此类基于语义的不可控威胁，必须在主机端侧实施持续攻击面管理，通过沙箱强制收敛智能体运行环境，严格遵循最小权限原则，对文件系统与本地指令的执行权限进行物理与逻辑双重隔离。

从网络接入角度，智能体的新型非人身份（NHI）伪造，绕过现有机器身份认证机制和访问控制截止。传统IAM体系（如基于角色的访问控制，RBAC）的设计假定了“人机交互”或确定性“机机交互（如静态API调用）”的交互模式，其认证主体通常为终端设备、员工账号或固定组织部门，权限策略可被预先定义并静态执行。同时智能体在执行任务过程中，其安全边界会随上下文动态变化，难以用预设策略完全覆盖。导致难以判别智能体的某一具体行为究竟是人类意图的合法授权委派，还是攻击成功后注入的恶意操作。其次智能体动态东西向流量剧增，传统南北向静态边界安全失效。因此需要新的面向智能体的新型身份治理与接入控制方案，实现对智能体细粒度的接入控制与东西安全访问控制。

从南北向边界防护视角来看，传统防火墙基于用户身份（IP地址）与应用特征（流量特征）进行管控，无法有效防御基于语义的运行时攻击。同时，AI能够自主发现漏洞并自动调用攻击工具，使得静态规则和人工预设的传统防护策略完全失效。由大语言模型驱动的智能体（LLM+Agent）其攻击能力已超越顶级黑客，可实现7×24小时持续自主攻击。因此，必须构建以AI对抗AI的主动安全防护体系。

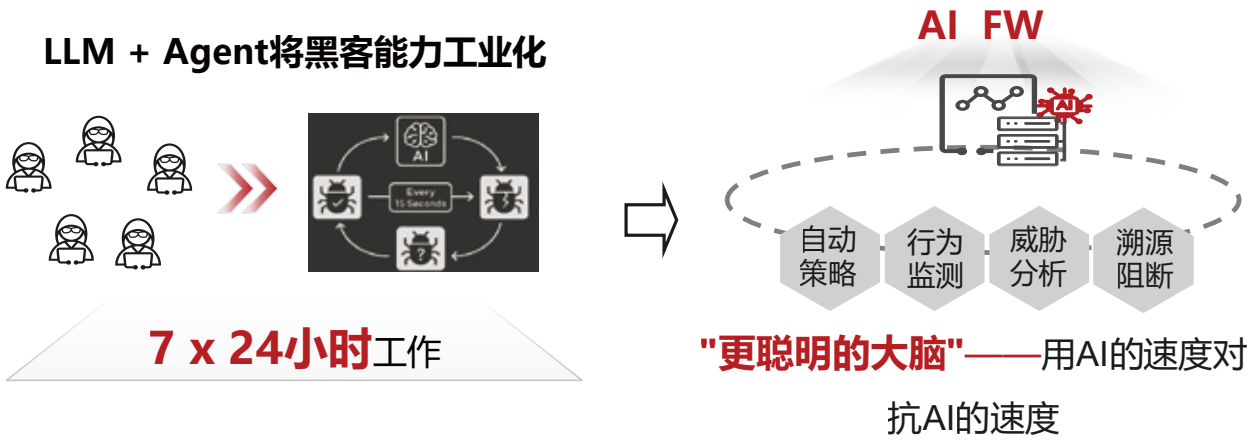


图 25 智能体网络时代需要AI对抗AI

6.2 智能体局域网目标网

智能体交互范式的变革，推动网络体系在三个核心维度发生根本性演进：1）分布式交互架构演进：企业技术栈由传统的“中心化单点调度”重构为基于多智能体系统（MAS）的分布式控制平面，通信范式从确定性的人机指令交互演进到智能体间（A2A）的自然语义交互；2）基于语义的动态转控分离架构：网络从静态连接模式，演进到基于智能体连接意图驱动的动态调度模式，基于智能体语义进行最优路径、最优性价比、最高服务质量的路由跳读；3）基础设施与网络底座层面演进：网络接入实体从静态终端变为具备自治能力的智能体，网络不再是传统的“数据透明传输管道”，网络成为能够深度解析业务意图、智能动态调度算网资源，提供确定性SLA与安全保障的“智能互联中枢”。

6.2.1 智能体局域网核心特征

智能体局域网的五大核心特征是“智能、开放、安全可信、极速超宽、确定性体验”，通过网络原生智能、开放协同、安全内生、高性能承载和确定性保障，构建面向未来智能体时代的新型网络基础设施。

1. 智能

核心特征： 网络原生智能、意图驱动、算力网络与安全融合。

智能体局域网络通过引入网络原生智能能力，实现从“连接驱动”向“意图驱动”的演进，以业务目标和智能体意图为核心，动态感知、理解和编排网络资源；同时深度融合计算、网络与安全能力，实现算力资源、网络能力和安全策略的一体化协同。

核心价值： 构建基于意图驱动的智能体网络，实现从业务需求理解、资源调度、策略生成到运行优化的全流程自动化闭环，最大化释放智能体生产力，支撑复杂智能应用规模化运行。

2. 开放

核心特征： 统一智能体通信协议、能力描述标准与开放交互接口。

面向多智能体、具身智能体协同场景，构建标准化的智能互联体系，通过统一通信协议、能力描述、交互接口规范，实现智能体能力可发现、可调用、可组合和可扩展。

核心价值： 打破异构系统间的生态孤岛和技术壁垒，形成开放、标准、可组合、可交易的智能体服务体系，推动异构智能体实现跨平台、跨领域、跨组织的高效协同，加速智能应用生态繁荣。

3. 安全可信

核心特征： 业务可追溯、接入可管控、传输零泄露、安全能力内生。

智能体局域网络将安全能力深度嵌入网络架构，实现从身份认证、访问控制、数据保护到行为审计的全生命周期安全管理，保障智能体交互过程中的可信运行。

核心价值： 构建“身份可信、行为可信、数据可信、治理可信”的安全可信体系，实现智能体通信、调用和协作过程的全链路可验证、可追溯、可治理，为智能体规模化应用提供安全底座。

4. 极速超宽

核心特征： 超高带宽、海量智能体高性能语义寻址、毫秒级低时延；算网存融合提升TOKEN生产效率。

面向大规模智能体并发接入和实时交互需求，智能体网络提供高吞吐、高并发、高效率的通信能力，通过语义级网络寻址提升智能体发现与连接效率。

核心价值： 支撑海量智能体实时协作与高性能通信，满足大模型推理、多模态内容生成、数字孪生实时同步等高带宽业务需求，实现端到端毫秒级低时延体验，保障智能应用高效运行；算网存融合实现智能体Token生产效率翻倍。

5. 确定性体验

核心特征：跨层协同应用感知、无损传输、毫秒级差异化业务调度。

通过确定性网络技术体系，实现对智能体业务需求的精准识别和网络资源动态保障，为不同类型、不同优先级、不同可靠性要求的智能体提供差异化服务能力。

核心价值： 打造可量化、可承诺、可保障的智能体网络服务模式，为关键任务型智能应用提供稳定可靠的网络体验，实现从“尽力而为”向“确定性交付”的网络能力升级。

6.2.2 智能体局域网目标架构

智能体目标网络包含四个层次，智能体网络应用层、智能体网络管控层、智能体网络连接层、智能体网络物理层。

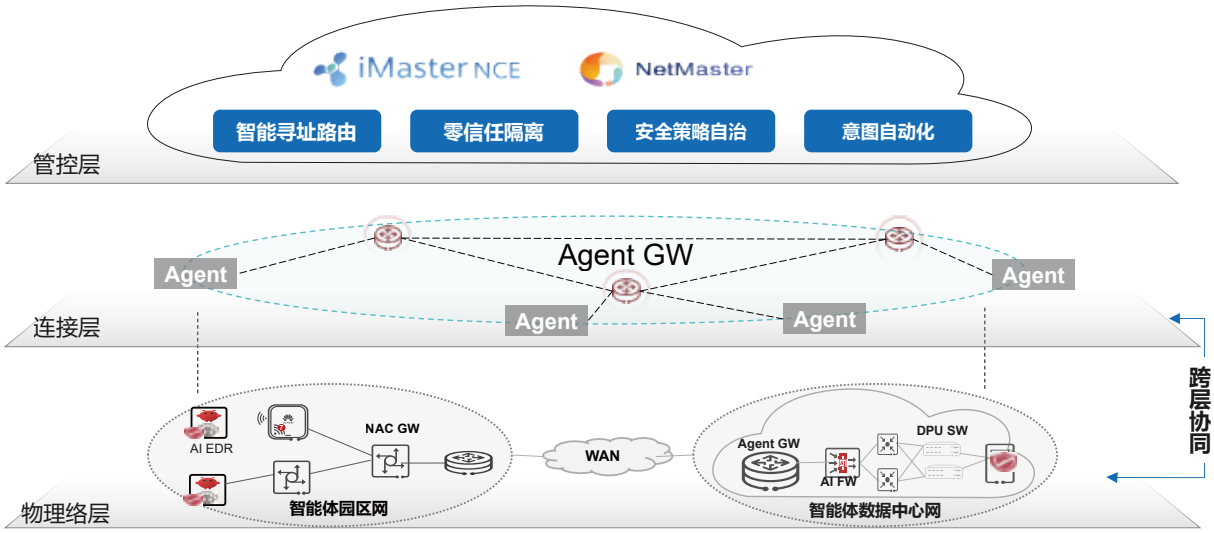


图 26 智能体局域网目标架构

1.智能体网络应用层

面向智能的设计、构建、测试、部署和运维提供化一站式作业平台。

- 智能体构建与设计：1）集成多种主流大模型（QWEN、DeepSeek、盘古等），用户可以根据任务需要灵活选择和切换；2）对于复杂的任务，提供低代码或者拖拽方式多智能体交互流程设计能力；3）提供长、短期记忆能力。短期记忆使得智能体能理解多轮对话的上下文；长期记忆则通过向量数据库存储用户偏好和历史，实现个性化服务。
- 智能体运维与管理：1）提供可视工具，能实时查看智能体的“思考”过程、调用了哪些工具、消耗了多少Token等，方便定位问题，2）提供仪表盘，实时监测智能体的调用量、响应时间、成功率等关键指标。

2.智能体网络控制层

智能体控制层主要提供智能体NHI身份管理、身份安全认证与动态发现，及智能体可观测、可审计能力。

- 智能体NHI身份管理：
  - NHI身份管理：智能体网关负责智能体NHI全局唯一标识分配以及对智能体的元数据的管理，包含智能体核心功能的语义化描述、授权智能体使用的工具集列表，以及智能体遵从的通信协议、输入输出（I/O）接口规范等。
- 智能体安全认证与动态发现：
  - 身份认证：园区网网络/数据中心网络侧提供严格的智能体身份校验机制，防范恶意或伪造的智能体节点接入智能体局域网。

  - 动态发现：园区智能体网关/数据中心智能体网关支持基于语义的智能体检索能力。通过解析自然语言意图，可动态匹配并推荐最满足当前业务场景的智能体。
- 智能体可观测与可审计：
  - 可观测与可审计：端侧AIDR与园区智能体网关/数据中心智能体网关联动，构建端到端（E2E）的立体监测与审计体系。针对智能体的业务行为数据、工具调用行为路径（Tool Use）以及大语言模型（LLM）的交互记录，提供高精度的数据留存与访问追溯能力，确保所有操作皆可审计、可溯源。

3.智能体网络连接层

智能体连接层提供智能、开放、安全可信的智能互联能力，旨在构建跨云、跨域、异构环境下智能互联底座。它向下屏蔽底层计算、网络环境差异，向上提供标准化、可重构的智能互联能力；同时，通过深度融合网络与安全能力，实现对智能体业务的自主安全防御，确保智能体交互的安全可信。

- 统一标准与多协议适配
  - 针对异构多模态智能体、跨混合云/多公有云平台、以及边缘分布式（多地多中心）的复杂部署场景，依托智能体网关抽象出统一的通信协议栈与语义交互接口规范。通过服务发现、统一寻址，实现异构智能体能力的全局可感知、动态调用。
- 网络安全协同的自主安全防御体系
  - 网络安全联动与微隔离：将安全防护延伸至网络边缘和智能体端侧。通过端侧AIDR（AI检测与响应机制）与网络的深度协同，提供基于身份、环境及意图的动态准入与访问控制。端侧AIDR、智能体网关与网络协同联动，联合构筑涵盖“模型层-Agent层-应用层-主机层-意图行为层”的五维立体安全内生围栏，阻断外部越权穿透，从根源解决智能体因“幻觉”或恶意攻击引发的行为失控风险。
  - 全链路（E2E）行为可视：端侧 AIDR、智能体网关及网络侧联动，实现智能互通流量、智能体行为全息可视，确保智能体端到端行为链上下文 100% 被记录与审计。支持高精度多维溯源，精准定位至“人、智能体、网络位置”。 基于“端侧AIDR - 智能体网关 - 网络层”三位一体的遥测（Telemetry）架构，对智能体间的互通流量、语义交互及调用行为行为路径进行全量记录。确保智能体端到端行为链的100% 留痕与可信审计。结合大数据与全链路拓扑分析，实现安全事件的秒级高精度溯源，精准定位至“自然人、具体智能体、物理/逻辑网络位置”。
  - 智能自主防御：基于E2E行为可视，实现智能体互访关系自主学习及安全风险的动态识别，实现安全策略的动态生成与秒级下发，对网络侧与智能体端侧的潜在风险进行实时拦截与阻断。基于全链路行为可视数据，自主学习智能体间的互访关系并建立安全基线，实现对异常行为与未知威胁（0-Day攻击）的实时、动态识别。通过控制层实现安全防护策略的自动生成与毫秒级下发，对网络侧与端侧的潜在风险实施实时拦截与阻断。

4.智能体网络物理层

智能体网络物理层目标提供极速超宽、确定性体验的面向智能互联的网络，实现百万级智能体并发接入、异构互通百毫秒语义寻址与高突发零丢包，通过网络调度提供端到端确定性SLA保障。

- 极速超宽网络，支持百万智能体并发接入

  智能体局域网需具备支撑百万级智能体同时在线与高密并发请求能力，实现异构智能体互通百毫秒语义寻址（准确率99%），并在高吞吐、高突发流量负载下确保网络零丢包。算网存融合避免CPU和内存带宽瓶颈导致IOPS和时延，精准拥塞控制解决多个DPU到1个NPU拥塞问题，避免存储IO流争抢带宽导致尾时延问题，实现TOKEN生产效率翻倍。

- 端到端确定性体验，不同业务提供差异化SLA保障

  通过物理层与连接层的跨层协同，实现应用感知网络以及毫秒级差异化业务调度等技术，构建确定性流量调度能力。通过对智能体交互意图与流量特征的线精准识别，网络可实现毫秒级的动态资源调配。基于网络硬切片隔离与确定性调度算法，为不同业务类型、不同优先级、不同丢包容忍度的智能体业务流，提供差异化SLA网络调度，确保关键核心业务（如金融级交易体、工业级控制体）在任何网络状态下都能保障“确定性低时延、确定性抖动、确定性带宽”的极致体验。

6.3 智能体局域网络企业园区

6.3.1 智能体局域网应用场景

金融企业网络普遍采用“总部园区、一级分行、二级分行、营业网点”的多层级广域互联架构，智算算力通常集中部署于主数据中心。分支园区常承载数千乃至上万员工的Wi-Fi办公接入，假定未来人均承载10个以上智能体，若分支侧无本地算力，所有智能体推理请求均需经广域网回传至主数据中心，将引入以下三类核心挑战：

智能体身份与访问控制缺失：当前缺乏面向AI智能体的统一身份认证与细粒度授权机制，难以有效识别并阻断未授权的“影子智能体”，无法防范私接、仿冒及权限滥用，违背零信任安全原则。

智能体引入新型攻击面与运行时风险：智能体基于语义的交互模式带来了全新的攻击面，传统防火墙与入侵防御系统无法检测和控制其运行时语义行为，可能导致越权数据访问、指令注入后的横向移动等攻击，使静态安全策略完全失效。

集中算力部署引发的端到端高延迟挑战：智能体交互对时延高度敏感。实测数据表明，营销类智能体每增加1秒延迟，客户流失率上升27%；而2–5秒的延迟会导致67%的用户放弃AI服务并转向人工客服。

智能体系统观测性面临挑战：首先，智能体高度的自主决策与执行机制使其运行逻辑呈现“黑盒化”特征，导致细粒度的行为合规审计与决策合理性难验证；其次，智能体间通信链路长且拓扑复杂，网络丢包、时延等劣化问题对智能体业务影响严重；最后，智能体架构中频繁的跨层数据流转与系统交互，导致故障溯源与安全事件的定责定界极其困难。

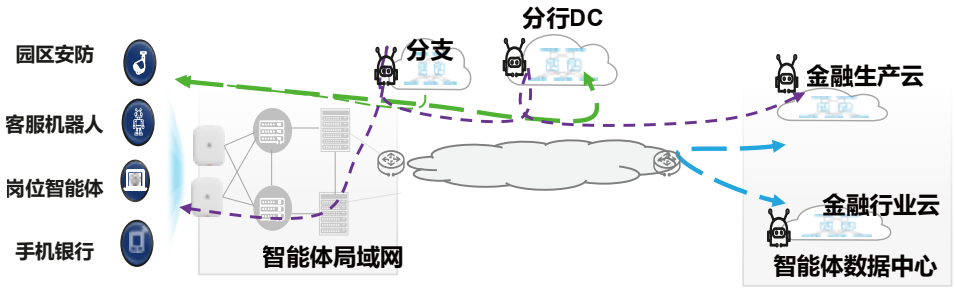


图 27 企业分支网点、分行、总行智能体交互

6.3.2 企业智能体园区网目标解决方案

通过“园区智能体网关+高性能Wi-Fi接入+端侧AI检测与响应（AIDR）”的联合防御体系，可实现以下纵深防护能力：

全量智能体实时发现与标记：对网络内全部智能体实例（含企业自建及xClaw等第三方智能体）进行实时感知与自动识别，资产覆盖率达100%，从智能体上线到被发现时延不超过5秒，所有智能体均被即时标记并纳入统一安全策略管理。

强制身份认证与链路层准入控制：任何智能体接入内网前，必须经过基于身份凭证的强制认证。未认证或认证失败的流量，直接在数据链路层被丢弃，实现端口级准入控制，杜绝未授权智能体私接与仿冒。

基于最小权限的动态微隔离：每个智能体仅被授权访问完成其任务所需的最小权限与网络端口集合，执行严格的应用层最小权限策略。任何超出授权基线的访问企图（涵盖东西向、南北向流量），均在50毫秒内被动态微隔离策略实时阻断，有效遏制横向移动与越权访问。

全量操作审计与攻击链溯源：针对每个智能体的每次操作（调用工具、访问目标资源或协作智能体等），均生成不可篡改的审计日志，并支持快速回溯，完整还原操作调用链，满足事件溯源与取证要求。

全域流量深度内容检测与语义分析：对Agent-to-LLM、Agent-to-Agent、Agent-to-MCP Server、Agent-to-APP等所有通信交互进行全量解密与深度包检测，覆盖加密流量与AI模型参数。通过内容级检查与上下文语义分析引擎，实现恶意代码及攻击载荷拦截率不低于99.99%。

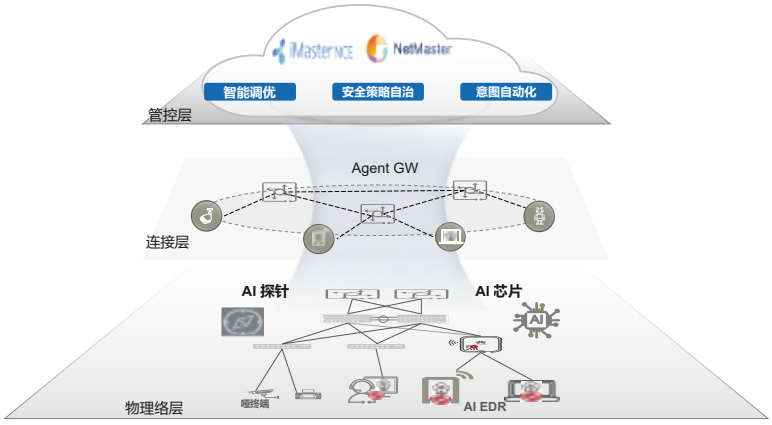


图 28 企业园区智能体目标网

主要功能部件包括：端侧AI EDR、园区接入交换机/WI-FI及新一代园区智能体NAC网关：

AI EDR实现智能体资产感知及非法意图阻断能力：首先，依托持续的攻击面管理，系统对进程树、系统调用序列及内存空间等底层主机资产进行全息遥测与漏洞动态评估，基线化风险暴露面；其次通过动态学习运行时（Runtime）行为基准，实时生成并下发内核级最小权限管控策略，实现细粒度的微隔离；最后建立端到端（E2E）的立体化全链路观测域，对Agent决策、大模型（LLM）推理及外部工具（Tools）调用的执行流进行意图关联与语义分析，从而精准识别复杂交互场景下的异常越权操作，全面保障AI原生应用的安全与合规。

园区接入交换机/WI-FI提供无损并发承载与零信任边界管控的深度融合：从网络并发和容量角度，边缘网络具备对多智能体流量的感知与精准识别能力，基于AI的主动式调度机制与动态QoS保障，实现在复杂高密环境下并发通信提升100%；在安全防御维度，基于零信任网络接入架构并将策略执行点下沉至网络边缘，不仅实现对Agent南北向流量、东西向流量的隔离防护，同时支持基于智能体数字身份标识，支持任务级的微隔离。

园区智能体NAC网关实现高性能转发、高并发认证、精细化体验保障一体集成：支持动态更新Agent安全访问策略，具备万级（10K）规则匹配处理能力，并且转发性能损耗控制在10%以内；高性能认证机制支持每秒千级（1000+）用户并发接入认证，并实现影子Agent的100%识别；同时提供智能体任务的全链路可视化管控，能够对推理业务的首帧响应时间（TTFT）及端到端处理耗时（TPOT）等核心体验指标进行实时监测与闭环管理。

7 技术展望与产业发展倡议

7.1 产业发展现状

当前面向智能互联的网络的发展呈现出明显的上下层分化态势。在应用层，生态发展正在加速繁荣，开源社区在此阶段扮演了核心的引领角色。以Google和Anthropic分别将A2A（Agent-to-Agent）协议捐赠给Linux基金会，并成立了A2A/AAIF开源社区为典型代表，其联合了众多行业巨头，通过定义通用的智能体名片（Agent Card）、基于 JSON-RPC 的交互范式及全生命周期管理，成功打破了不同智能体开发框架之间的生态烟囱，实现了上层的语义发现与能力协商。与此同时，配合 Anthropic推出的MCP（Model Context Protocol）协议，应用层已初步具备了跨厂商工具调用与数据打通的能力。

然而，尽管应用层的技术迭代如火如荼，底层的数通网络基础设施却面临着严重的“管道化”瓶颈。目前的产业探索仍普遍将底层网络视为“透明管道”，随着常驻智能体和自主并发任务呈指数级爆发，完全依赖 HTTP/HTTPS 等传统应用层协议进行交互，正面临着群组传输效率低下、跨域安全难控等严峻挑战。虽然业界已开始意识到这一断层并展开网络层面的初步尝试，但网络基础设施如何原生提供大规模智能体通信支持，尚未得到产业界的足够重视。智能互联协议栈的下沉与网络底座的系统级重构，亟需业界投入更多的研究力量与产业资源。

7.2 技术发展展望

面向智能互联的长期发展愿景，现有以应用层协议和平台为中心的技术体系将难以支撑未来海量智能体的高频协同需求。未来的技术演进方向，应逐步从应用层能力叠加（Overlay）向网络基础设施内生能力演

变，将智能互联所需的发现、路由、身份、安全以及协同等核心能力逐步下沉到网络层，构建面向智能体时代的新型网络基础设施。

首先，语义路由（Semantic Routing）将成为未来的重要研究方向。传统IP网络仅依据地址进行数据转发，而智能体之间的交互更多围绕任务目标、服务能力和上下文语义展开。未来网络需要突破基于地址的静态寻址模式，在网络基础设施中逐步具备对智能体多模态意图、能力描述及动态上下文的理解能力，实现面向任务的智能发现与语义路由。例如，网络能够根据"寻找具备医学影像分析能力且位于低时延区域的智能体"等高层语义请求，自动完成能力匹配、路径选择和服务发现，从而提升跨域智能体协作效率。这种由"地址驱动"向"能力驱动、语义驱动"的演进，将成为面向面向智能互联的网络区别于传统互联网的重要特征之一。

其次，面对未来全球范围内可能达到千亿级规模的智能体协同，网络原生的海量消息分发能力将成为支撑面向智能互联的网络规模化发展的关键基础设施。目前，大规模智能体消息交换主要依赖应用层消息中间件或云平台实现，在跨地域、高并发场景下容易形成性能瓶颈。未来应充分利用智能网卡、可编程交换芯片等硬件加速能力，在网络层原生支持智能体消息流的高效转发、组播通信、异步消息总线、发布/订阅等通信模式，实现海量智能体消息的线速处理和低开销分发。同时，结合广域网络QoS调度、流量工程以及边缘协同机制，可进一步降低跨地域通信时延，提高智能体集群协同效率，为大规模分布式智能体系统提供可持续扩展的通信基础。

与此同时，分布式内生信任体系也将逐渐扩展传统集中式认证中心的信任模式和能力边界。在智能体网络中，大量智能体跨越组织、运营商乃至国家边界动态协作，传统集中式证书体系难以满足高动态、高频认证以及跨域信任建立的需求。未来可依托可信执行环境（TEE）、硬件密码模块、可信平台模块（TPM）等硬件可信根，在网络层构建原生的分布式身份认证体系，实现智能体之间的双向身份验证、端到端数据加密、远程证明以及可验证凭证（Verifiable Credentials）的分布式处理，使信任能力成为网络基础设施的内生组成部分，而非依赖应用层重复构建。

最后，网络对上层应用做质量保障的“传统强项”也将继续发展，实现智能体交互感知的自适应流控与拥塞控制。智能体网络流量具有极强的突发性、密集的同步协同性（如多智能决策等场景）。未来网络需构建智能体行为感知的流控机制，网络节点通过深度报文解析或行为模式识别，能够识别出智能体任务强相关与普通的数据负载，进而做差异化的保障。在网络发生瞬时拥塞时，优先保障任务相关报文的零丢包与超低时延传输，防止因某一个协同智能体的报文丢失而导致整个多智能体集群系统发生性能塌陷。

总体而言，未来面向智能互联的网络的发展，不应局限于在现有互联网架构之上增加新的应用协议，而应推动网络基础设施从"连接设备"向"连接智能体"演进，从"传输数据"向"支撑智能协作"演进，使网络逐步具备语义理解、可信协同、智能调度和自治运行等原生能力，为万物智联时代构建更加高效、安全、开放的新一代网络体系。

7.3 产业发展倡议

面向智能互联的网络的发展，不仅依赖于大模型能力的持续提升，也需要网络基础设施同步演进，形成"

智能体+网络"协同发展的新范式。面对未来海量智能体跨组织、跨网络、跨地域协同的发展趋势，仅依靠单一厂商或单一领域的技术创新，难以构建开放、统一、可持续发展的智能互联生态。

为此，本白皮书倡议产业界加强协同创新，推动网络基础设施与智能体技术的深度融合。建议国际和国内标准组织、网络设备厂商、电信运营商、云服务提供商、智能体平台、科研机构以及行业用户等各方，打破传统网络、云计算、人工智能和应用平台之间的技术边界，围绕面向智能互联的网络体系架构开展联合研究，共同推动关键技术、接口协议和标准体系的统一演进。

重点围绕智能体发现与寻址、身份认证与可信入网、智能体网关、语义路由、群组通信、广域网QoS保障、跨域协同、安全治理等关键基础能力，推动形成开放兼容、互联互通的技术体系，避免智能体生态碎片化和重复建设，为不同厂商、不同平台之间的智能体互操作奠定统一基础。

同时，鼓励产业各方加强试点验证和开放生态建设，通过建设跨运营商、跨云平台、跨行业的示范应用和互联测试环境，加快推动相关技术从概念验证走向规模化部署，促进标准、产品、网络和应用协同成熟，逐步形成覆盖全球的智能互联基础设施。

展望未来，面向智能互联的网络的发展不应局限于在现有互联网之上构建新的应用平台，而应推动智能互联能力逐步由应用层向网络基础设施层延伸，使网络具备智能体发现、可信连接、高效通信、安全治理和智能协同等原生能力，共同构筑一张高性能、高可信、开放互联、可持续演进的全球面向智能互联的网络基础设施，为下一代互联网的发展提供坚实支撑。

8 结语

当前，人工智能正从单体智能向多智能体协同的群体智能加速演进，构建公平、普惠、高效、可信的面向智能互联的网络，已成为全产业的普遍共识与迫切需求。本白皮书聚焦异构智能互联互通这一行业核心痛点，系统优化了包含全层级安全与可观测能力的面向智能互联的网络四层总体架构，创新提出智能互联局域网、广域网的分层分域场景划分；围绕可信入网核心命题，建设性提出 “中心拓展 + 分布式执行” 的智能体身份与注册管理体系，明确了以智能体网关承载执行节点的分布式一体化架构，清晰界定了智能体网关作为传统网络到智能体网络的衔接桥梁、分布式认证节点、安全与效率载体的核心基础设施定位。报告同时通过家庭智慧康养、2家3代人、金融、教育等典型场景的落地实践，验证了多智能体协同的产业价值，并从标准体系建设、技术融合创新、产业部署落地等维度给出了体系化行动指引。

面向智能互联的网络是支撑 AI 产业规模化发展的下一代数字基础设施，是打通端网云生态壁垒、释放群体智能生产力、赋能千行百业数字化转型的核心底座，其发展不仅将重塑数字产业生态格局，更将为数字经济持续增长注入全新动能。

面向智能互联的网络的建设是一项系统性工程，离不开产业界、学术界、政策与社会各界的协同共建。我们呼吁产业各方凝聚共识，以开源共建模式推动标准体系落地，加快试验网部署与场景创新，把握行业标准与国际标准制定主动权；呼吁学术界持续攻坚基础理论与关键技术，为产业演进提供源头支撑；呼吁监管与政策部门完善制度框架，营造可管可控、健康有序的发展环境。期待各界携手同行，共同推动面向智能互联的网络的技术迭代与产业繁荣，共创智能协同的数字未来。

缩略词

缩写	英文全称	中文名称
QoS	Quality of Service	服务质量
RAG	Retrieval-Augmented Generation	检索增强生成
BNG	Queries Per Second	每秒查询率
P2P	Broadband Network Gateway	宽带网络网关
NP-hard	Non-deterministic Polynomial-hard	非确定性多项式困难问题（NP难问题）
TCP	Transmission Control Protocol	传输控制协议
QUIC	Quick UDP Internet Connections	快速 UDP 互联网连接
RL	Reinforcement Learning	强化学习
CDN	Content Delivery Network	内容分发网络
A2A	Agent to Agent	智能体间交互
MCP	Model Context Protocol	模型上下文协议
ANP	Agent Network Protocol	智能体网络协议
ACP	Agent Communication Protocol	智能体连接协议
IETF	Internet Engineering Task Force	互联网工程任务组
RBAC	Role-Based Access Control	基于角色的访问控制
API	Application Programming Interface	应用程序编程接口
DID	Decentralized Identifiers	去中心化标识符
VC	Verifiable Credentials	可验证凭证
IAM	Identity and Access Management	身份与访问管理
NAC	Network Access Control	网络访问控制
WAF	Web Application Firewall	Web 应用防火墙
AI	Artificial Intelligence	人工智能

缩略词

缩写	英文全称	中文名称
ANI	Agent Network Infrastructure	智能体网络基础设施
C/S	Client/Server	客户端 / 服务器架构
B/S	Browser/Server	浏览器 / 服务器架构
NHI	Non-Human Identity	非人类身份
IOA	Internet of Agents	面向智能互联的网络
TTFT	Time To First Token	首令牌生成时间
RTT	Round-Trip Time	往返时延
PKI	Public Key Infrastructure	公钥基础设施

商标声明

和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址：深圳市龙岗区坂田华为总部办公楼

邮编：518129

网址：https://www.huawei.com

客户服务邮箱：support@huawei.com

客户服务电话：4008302118