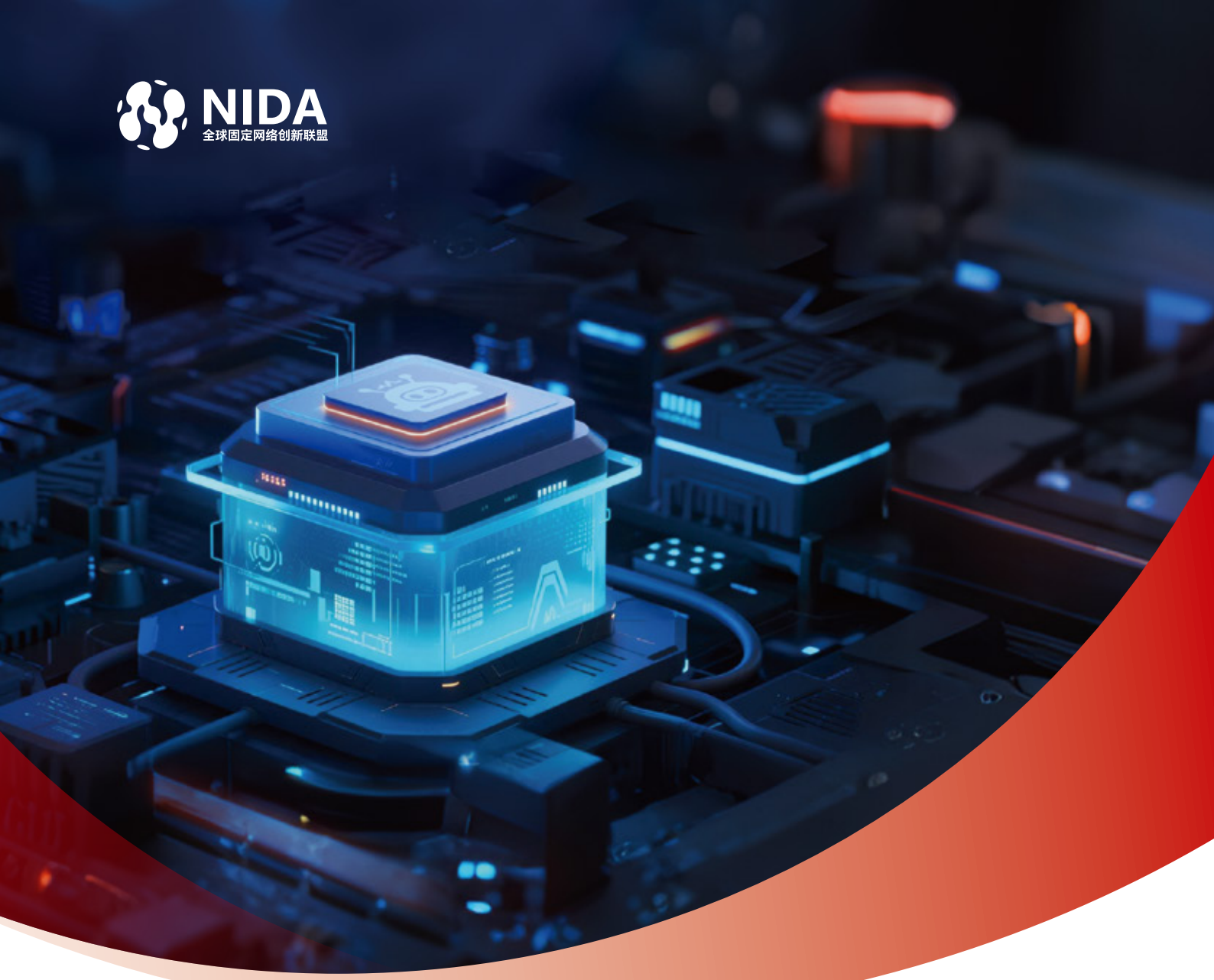
NIDA
全球固定网络创新联盟



AI Agent

通信网关技术研究报告

前言

随着人工智能技术的飞速发展，多智能体系统在各个领域得到了广泛应用，例如智能交通系统中的车辆协同调度、工业自动化中的机器人协作、复杂商业流程中的智能决策支持等。多智能体系统通过多个智能体之间的协作，能够高效地解决复杂的任务，展现出巨大的潜力。

然而，多智能体系统在实际应用中面临着诸多挑战。首先，智能体之间需要高效的通信机制以确保信息的快速传递和准确交互。其次，智能体可能来自不同的框架、平台或组织，需要解决通信协议的兼容性问题。此外，智能体之间的协作需要安全机制来保障数据的保密性和完整性，防止未经授权的访问和数据泄露。最后，随着系统的扩展，系统的可扩展性和性能优化也变得至关重要。

为了应对这些挑战，AI Agent通信网关应运而生。AI Agent通信网关是一个专门设计的平台，用于管理、协调和优化多智能体系统中的通信和协作。它充当智能体之间的通信枢纽，提供标准化的接口和协议，使得来自不同框架、平台或组织的智能体能够无缝地进行交互。通过AI Agent通信网关，智能体可以高效地交换信息、协同工作，共同解决复杂的任务。

本文件起草单位：中国信息通信研究院、华为技术有限公司、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、中国联合网络通信有限公司研究院。

本文件主要起草人：曹畅、高巍、胡泽华、金剑、刘鹏、宋健、曾冠铭、朱科义、朱永庆。

*注：本文件起草单位和主要起草人排名不分先后。

目录

1 AI Agent 通信网关：AI Agent 演进趋势下的关键基础设施

1.1 AI Agent 的发展现状

根据 Anthropic 的定义，AI Agent 是一种能够使用大型语言模型或其他人工智能技术来完成任务的系统[1]。它可以是完全自主的系统，能够在较长时间内独立运行，使用各种工具来完成复杂任务，也可以是遵循预定义工作流的更规范的实现。

AI Agent 已广泛应用于多个领域。具体表现在：

- 在客户服务领域，AI Agent 能够实时响应客户咨询、提供精准解答，提升客户满意度。
- 在智能家居领域，AI Agent 作为核心控制单元能够整合各类智能设备，实现设备协同工作。
- 在自动驾驶领域，AI Agent 通过环境感知、实时决策和路径规划，为自动驾驶汽车提供核心技术支持。
- 在 AI 游戏领域，AI Agent 为游戏设计提供更智能的非玩家角色行为和动态游戏环境。
- 在金融、零售和医疗保健等专业领域，AI Agent 的应用也在不断深化，能够分别作用于风险评估、个性化推荐和辅助诊断等方面。

随着人工智能技术的不断进步，AI Agent的能力和性能得到显著提升。大模型的发展为AI Agent带来了通用任务解决能力和自然语言交互界面，AI Agent能够通过感知环境、推理决策来完成任务，利用传感器获取环境信息，并通过机器学习算法和逻辑推理引擎进行分析处理。

据报告显示，越来越多的组织计划在未来实施AI Agent。据Gartner预测，到2028年，至少有15%的日常工作会被生成式AI取代[2]。AI Agent在未来几年将得到更广泛的应用和推广。面向未来，AI Agent将从被动的助手转变为积极的问题解决者，能够提供超个性化体验、发展更好的情商、具备多模态能力，并与物联网和设备深度集成。

1.2 AI Agent 通信网关的概念和功能

随着人工智能技术的飞速发展，多智能体协同在各个领域的应用日益广泛。从智能交通系统中的车辆协同调度，到工业自动化中的机器人协作，再到复杂商业流程中的智能决策支持，多智能体系统展现出了强大的潜力。Internet of Agents（IoA，智能体互联网）是一种新型的框架，旨在通过开放协议和共享目标，使AI Agent能够彼此发现并协调行动[3]。它受到互联网架构的启发，旨在连接不同环境中的多样化AI代理。然而，这些系统面临着诸多挑战，如智能体之间的通信、协作、安全性和可扩展性等。AI Agent通信网关（AI Agent Communication Gateway）应运而生，作为连接不同智能体、实现高效协作的关键基础设施，它在智能体互联网中扮演着至关重要的角色。

1.2.1 AI Agent通信网关的定义

AI Agent通信网关是一个专为管理、协调和优化多智能体系统中的通信和协作过程而设计的平台。它可以充当智能体之间的通信枢纽，提供标准化的接口和协议，使得来自不同框架、平台或组织的智能体间能够无缝地进行交互。通过AI Agent通信网关，智能体可以高效地交换信息、协同工作，共同解决复杂的任务。

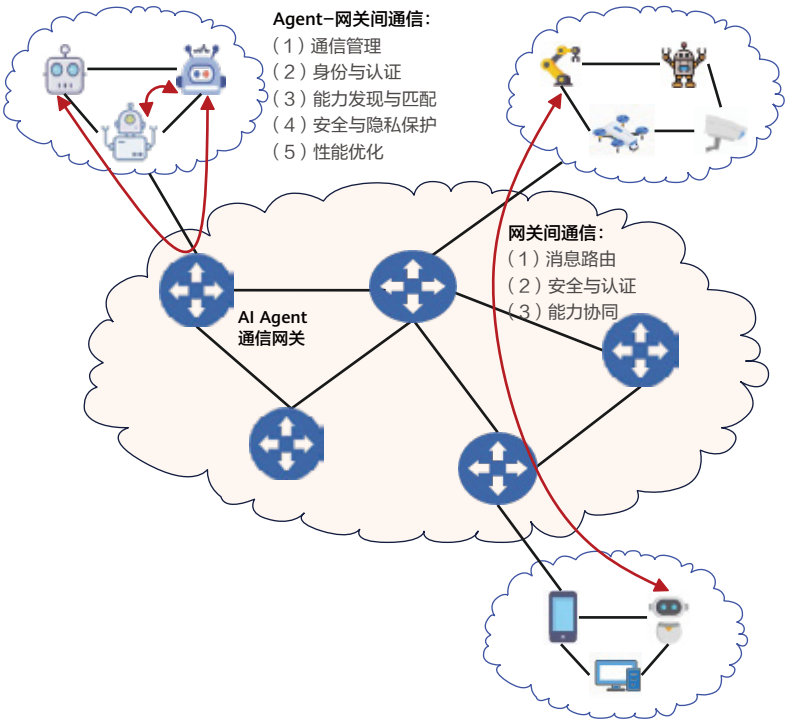


图2　AI Agent 通信网关组网与功能

1.2.2　AI Agent 通信网关与智能体间通信的核心功能

AI Agent 通信网关与智能体间通信的核心功能主要表现在以下五个方面：

通信管理

- **消息分发：**AI Agent 通信网关负责将智能体之间的消息高效地分发到目标智能体。它支持多种通信模式，包括请求–响应、发布–订阅、发后即忘和流式传输，能够满足不同场景下的通信需求。
- **协议适配：**智能体可能使用不同的通信协议，AI Agent 通信网关能够进行协议转换和适配，确保智能体之间的通信顺畅无阻。

身份与认证

- **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（在某些广域网场景下，Agent ID 也可以通过分布式 DID 等其他方式分配），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，AI Agent 通信网关能够控制智能体对资源的访问权限，保障系统的安全性。

能力发现与匹配

- **智能体能力描述：**AI Agent 通信网关允许智能体通过标准化的方式描述自身的能力，包括功能、特性、支持的通信模式等。这些能力信息存储在智能体目录中，供其他智能体查询。
- **动态能力匹配：**当一个智能体需要与其他智能体协作时，AI Agent 通信网关可以根据任务需求，从智能体目录中动态发现具有相应能力的智能体，并建立通信连接。这种方式使得智能体之间的协作更加灵活，能够根据实时需求动态调整协作伙伴。

安全与隐私保护

- **数据加密：**AI Agent 通信网关对智能体之间的通信数据进行加密处理，确保数据在传输过程中的保密性和完整性，防止数据泄露和篡改。
- **访问控制：**AI Agent 通信网关通过严格控制智能体对敏感信息和资源的访问，防止未经授权的访问和操作。同时，通过隐私保护机制，AI Agent 通信网关能够确保智能体在协作过程中不会泄露自身的隐私信息。

性能优化

- **负载均衡：**AI Agent 通信网关能够根据智能体的负载情况和系统资源的使用情况，合理分配通信请求，避免某些智能体过载，提高系统的整体性能和稳定性。
- **消息缓存与优化：**AI Agent 通信网关能够对频繁发送的消息进行缓存，减少重复计算和传输，提高通信效率。同时，通过优化消息的格式和传输路径，AI Agent 通信网关还能进一步提升系统的性能。

1.2.3 AI Agent通信网关通信的核心功能

在多智能体系统中，AI Agent 通信网关不仅负责管理单个网关内部的智能体通信，还需要与其他网关进行高效协作，以实现更大范围的智能体协同和资源共享。因此，AI Agent 通信网关之间的通信是多智能体系统中不可或缺的一部分，其核心功能主要体现在以下三个方面：

网关之间的消息路由

- **消息转发：**当一个 AI Agent 通信网关收到一个需要跨网关处理的消息时，该网关需要能够将消息正确地转发到目标网关。消息路由机制应能够根据目标智能体的 Agent ID 或任务需求，动态选择最佳的转发路径。
- **负载均衡与优化：**在多个AI Agent 通信网关之间进行消息转发时，需要考虑负载均衡，避免某个网关因处理过多消息而过载。同时，通过优化消息的传输路径和格式，可以减少传输延迟和资源消耗，提高系统的整体性能。

网关之间的安全与认证

在AI Agent通信网关之间的通信过程中，数据加密是必不可少的，通过加密技术，可以确保数据在传输过程中的保密性和完整性，防止数据被窃取或篡改；同时，隐私保护机制可以确保AI Agent通信网关在共享资源或协作过程中不会泄露自身的敏感信息。

网关之间的能力协同

- **能力发现与资源共享：**AI Agent通信网关之间可以通过能力发现机制，了解彼此所连接的智能体的能力和资源。当一个网关需要某种特定能力的智能体时，可以通过网关间的协作，从其他网关中动态发现并调用相应的智能体。
- **任务分配与协同处理：**对于复杂的任务，可能需要多个AI Agent通信网关及其连接的智能体共同协作完成。通过任务分配机制，可以将任务分解为多个子任务，并根据各网关的能力和负载情况，合理分配给不同的网关及其智能体，以实现高效的协同处理。

1.2.4 AI Agent通信网关的核心价值

AI Agent通信网关的核心价值主要体现在以下四个方面：

提升协作效率

通过标准化的通信接口和协议适配，AI Agent通信网关能够消除智能体之间的通信障碍，使得智能体之间的协作更加顺畅。同时，基于能力的动态发现和匹配机制，AI Agent通信网关能够根据任务需求快速找到合适的协作伙伴，提高协作的灵活性和效率。例如，在一个复杂的项目中，需要多个具有不同专业技能的智能体共同完成任务，AI Agent通信网关可以在短时间内找到这些智能体并建立通信连接，加快项目的进度。

增强系统安全性

AI Agent通信网关提供了全面的安全机制，包括认证、授权、数据加密和访问控制等。这些安全措施能够有效防止未经授权的访问、数据泄露和恶意攻击，保障多智能体系统的安全运行。在跨组织的智能体协作中，安全性尤为重要，AI Agent通信网关通过严格的认证和授权机制，确保只有合法的智能体能够接入系统，并且对敏感信息进行加密处理，保护组织的商业机密和用户隐私。

提高系统的可扩展性

AI Agent 通信网关的设计支持大规模智能体的接入和通信，通过负载均衡和消息缓存等机制，能够有效应对智能体数量的增加和通信流量的增长，保证系统的稳定性和性能。同时，AI Agent 通信网关的分布式架构和弹性伸缩能力，使其能够适应不同规模的应用场景，在从企业级的小型系统到跨组织的大型系统中都能很好地运行。例如，在一个智能城市项目中，随着城市规模的扩大和智能体数量的增加，AI Agent 通信网关可以动态调整资源分配，确保系统的正常运行。

促进智能体生态系统的构建

AI Agent 通信网关为智能体的开发和部署提供了一个统一的平台，降低了智能体之间的集成难度。开发者可以专注于智能体的功能开发，而无需过多关注通信和协作的细节。这有助于吸引更多的开发者参与智能体的开发，丰富智能体的种类和功能，促进智能体生态系统的构建和发展。AI Agent 通信网关作为连接这些智能体的桥梁，使得智能体能够在不同的应用环境中进行协作，推动智能体技术的广泛应用。

2 AI Agent 通信网关的应用场景

2.1 To H：家庭场景的 AI Agent 通信与组网

AI Agent 的广泛部署正在重塑未来家庭的智能网络架构。随着机器人、无人机、机器狗、智能家居终端、老年陪护设备和智慧教育助手等多种类型的 AI Agent 纷纷入驻家庭环境，家庭网络已经从传统的“终端接入”模式，演变为以“多 Agent 协同、自治通信与异构融合”为核心的新型架构。这对家庭网络的网关提出了全新的诉求与挑战。如图2所示是家庭场景的 Agent 网络，其中涉及的概念和技术将在子章节中进行描述。

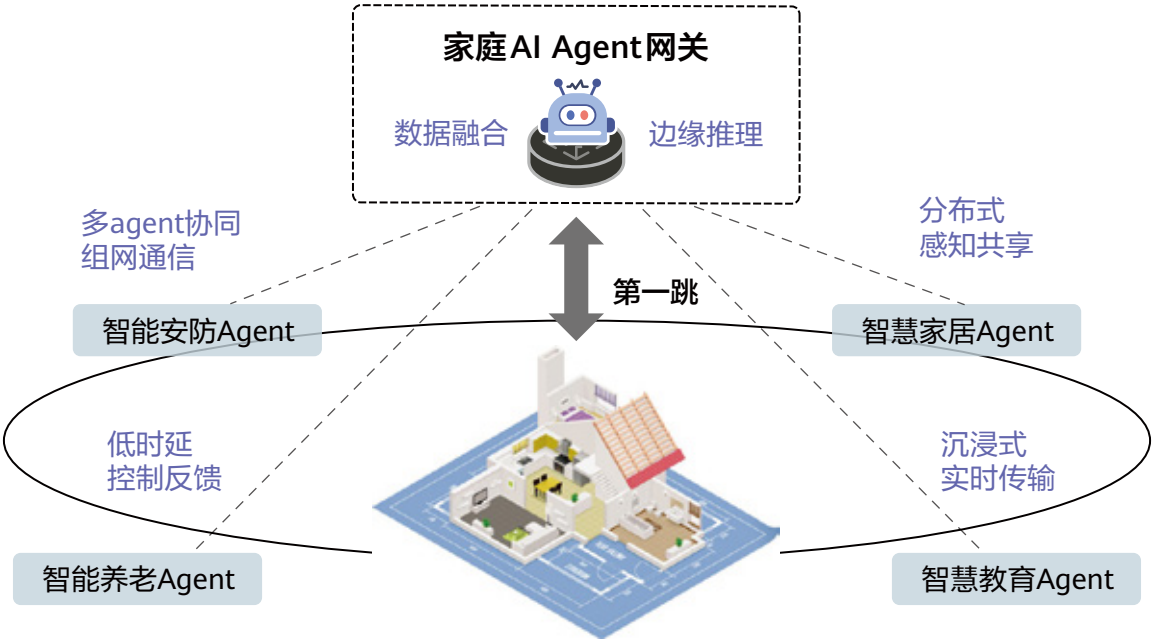


图2　家庭场景的AI Agent网络

2.1.1　家庭“第一跳”智能入口网关

家庭场景的AI Agent通信与组网具有多类型智能体协同和通信模式复合化这两大特点，需要AI Agent通信网关作为家庭“第一跳”的智能入口。两大特点的具体表现如下所述：

多类型智能体协同

- 服务型机器人（如扫地机器人、送物机器人）需要与语音助手、门锁、摄像头协同完成任务调度与信息同步。
- 无人机用于巡检、安防或远程喊话，其飞行控制和图像回传对时延和带宽要求极高。
- 机器狗具备一定的运动智能与环境感知能力，经常充当陪护或安防角色，与家庭主控Agent频繁通信。
- 智能家居终端（如空调、灯光、窗帘）主要通过语义控制方式与用户互动，接收来自中心Agent的统一调度。
- 老人陪护系统整合生理监测设备与语音交互机器人，要求数据的实时性与隐私保障。
- 智慧教育终端（如学习投影、AI学习助手）常常需要与家长的移动终端实时联动并对接云端大模型。

通信模式复合化

Agent之间的通信不再基于简单的“设备–云–控制端”模型，而是呈现出以下趋势：

- **边缘协同通信：**多个Agent可以直接进行P2P通信，无需每次绕行云端。
- **分布式感知共享：**如机器人与摄像头共享环境建图信息、多架无人机共享空气质量数据等。
- **低时延控制反馈：**例如，机器狗接收指令并及时回传状态，用于低时延反馈控制。

2.1.2 家庭AI Agent通信网关新要求

为了支持以AI Agent为核心的家庭智能系统，家庭网络网关需要演进为“AI Agent网络中枢”，应当具备以下五大关键能力：

高并发、低时延接入能力

- 支持上百个Agent级设备同时稳定在线，且保障QoS隔离（安防vs娱乐vs控制）。
- 提供基于Wi-Fi QoS调度机制的时延保障。

边缘计算与决策能力

- 集成轻量边缘推理能力，支持部分Agent（如机器人或摄像头）离线智能决策或中间感知融合。
- 内置“家庭中控智能体”，作为多个Agent的策略调度器和事件中心。

异构通信协议网关

- 提供Agent间的协议转换与命名服务支持，实现跨协议的发现与编排。

安全与隐私保障能力

- 支持本地数据存储与加密分析，避免隐私信息上传云端。
- 提供智能体访问控制策略管理（例如，机器狗不能访问智慧教育终端的数据）。

可编程与可管控性

- 家庭网关应提供可编程接口（如Agent服务注册、调度规则下发），支持用户自定义Agent行为逻辑。
- 支持拓扑感知与可视化，便于家长或管理员掌握当前Agent状态与通信图谱。

2.1.3 典型案例：家庭安防与智能助理协同

下面是一个典型AI Agent通信网关在家庭安防与智能助理协同场景中的应用案例。在家中部署了多个智能设备和AI Agent，包括智能摄像头、门磁传感器、安防机器人（如具备运动检测功能的机器狗）、智能语音助理以及中心AI家庭网关。这些设备具备Agent能力，或者能够通过MCP等协议为其他Agent提供功能调用。各智能设备和AI Agent间的协同流程示例如下所述：

入侵事件检测	晚上23:30，门磁传感器触发大门被异常打开的事件。中心网关接收到传感器数据后，立即唤醒摄像头与安防机器人。
感知与验证	摄像头快速抓拍并执行人脸识别，鉴定为陌生人。安防机器人启动UWB定位，快速移动到门口区域，发出现场语音警报。
信息融合与家庭提醒	先将所有数据流（图像、位置信息、事件日志等）汇聚到网关。网关经过分析后，控制语音助手在卧室内播放警告音：“检测到可疑人员靠近大门，是否报警？”。家庭成员通过语音确认：“立即报警。”。
后续动作控制	网关向云端报警平台发送信息并启动远程可视通话；同时，安防机器人持续跟踪陌生人移动轨迹并录像。

通过AI Agent网关的多Agent编排能力，在家庭场景中实现了从感知、判断到执行的完整闭环，在提升安防能力的同时，增强了人与智能体的自然互动。这样的网关不再只是“路由器 + 协议桥”，而是家庭智能行为的中控神经系统。

2.2 To B：跨组织数据流通与智能组网

企业的数字化进程正从“系统整合”转向“智能协作”，AI Agent正逐渐成为支撑企业内部流程自动化和跨企业生态联动的关键技术单元。相比传统API接口集成模式，AI Agent能够通过语义感知、策略驱动、自主决策等能力实现更加灵活、低耦合的协作方式。这一变化的本质，是将“数据共享”升级为“智能共享”，将“系统集成”升级为“智能体网络”。然而，要构建一个多Agent协同的可信通信体系，尤其是在多个企业或组织之间，必须重新思考网络基础设施和数据治理模型。

过去的企业间通信主要依赖静态配置的VPN、定制化接口或者B2B平台，这些方式存在连接刚性强、数据权限边界模糊、升级成本高等问题，不适合高度动态、智能化的Agent网络。为此，我们提出在云侧部署Agent Gateway（AGW）的方式，以此构建一套既可弹性连接、又可数据隔离的智能组网与通信平台。AGW不仅是连接多个Agent的网络枢纽，更是保障组织边界清晰、数据安全流通的策略中控，构建起一个“可信的智能体协作网络”。AGW需要具备以下两个核心能力：

- **智能服务注册与发现：**AGW支持多租户微服务注册，可根据Agent的角色、数据权限、延迟要求等进行智能调度与路径选择。
- **边界智能策略引擎：**AGW内置策略引擎用于实现组网时的认证授权、QoS保障和流量审计，确保跨Agent通信安全有序。

2.2.1 云侧部署AGW实现灵活组网

在现代企业中，AI Agent通常被部署在各个微服务系统内，服务于业务链的某一局部。例如，生产制造系统中的排产Agent、营销系统中的客户预测Agent、IT系统中的资源调度Agent等，它们之间需要进行跨应用甚至跨区域的通信才能完成端到端的业务闭环。而当Agent部署在多云、多VPC、甚至多组织的网络结构中时，如何实现高效、低延迟的连接，成为系统设计的核心挑战。

AGW正是在这一背景下应运而生，它位于企业云网络的逻辑边界，以服务网格或Sidecar形式对各Agent进行注册与编排。AGW通过构建动态Overlay网络，实现逻辑互通、物理隔离的虚拟Agent网络。其策略引擎可以根据Agent的任务类型、数据敏感等级、所处组织角色等要素，灵活决定其通信权限、路径优先级以及链路加密等级。这种方式极大地提升了Agent组网的灵活性，不仅支持临时协作型网络的快速构建，也支持长生命周期Agent的稳定运转。

与传统网络方案不同，AGW 并不以 IP 或 MAC 为组网单元，而是以“Agent 身份 + 任务类型”为主索引。这样使得网络不再与拓扑强绑定，而是转为以任务流和数据权限为导向的逻辑连接，实现了真正的“按需组网、策略驱动”的网络形态。这种设计特别适用于那些频繁变更任务编排、异构系统并存的企业环境，也为 Agent 自治行为留出了足够的策略弹性。

2.2.2 云跨组织通信中实现敏感数据“零泄漏”

当 AI Agent 间的协作跨越组织边界时，数据安全问题随之激化。企业往往面临两难选择：要么开放接口、牺牲部分数据主权；要么设置壁垒、牺牲协同效率。AGW 试图打破这一悖论，构建一种“数据不出域，智能来协同”的机制，使跨组织通信既安全又高效。

AGW 的安全模型不依赖于传统的“黑白名单”逻辑，而是构建在“可验证、最小授权、加密计算、全链路审计”这四个核心支柱之上。首先，任何 Agent 之间的通信都必须通过AGW 进行策略验证，只有通过了权限校验和上下文任务匹配，数据才会被授权进入“协同通道”。其次，AGW 使用数据裁剪与最小可用原则，仅允许目标 Agent 获取当前任务所需的最小数据子集，并自动加密所有传输内容。

更重要的是，AGW 支持基于同态加密、联邦推理和安全多方计算（Secure Multi-party Computation，SMPC）等新一代隐私计算技术，使得 Agent 即使无法访问原始数据，也能参与模型运行并获取有效的决策反馈。这种“计算可达，数据不可见”的范式彻底解决了数据主权与协作效率之间的矛盾。例如，一个医疗诊断 Agent 可以在不暴露患者信息的前提下，利用另一个医院的模型进行推理得到诊断建议；再如，一个制造商的计划 Agent 可以在不知晓供应商具体库存数据的前提下，协同进行物料计划。

AGW 还内建了全链路的行为审计机制，支持以区块链或不可篡改日志链的形式记录每一次跨组织的 Agent 通信行为，从身份认证、策略匹配、数据摘要、通信轨迹到任务完成状态，形成完整的责任链。这为未来的数据合规、风险回溯、智能体治理等提供了关键支撑。

2.2.3 典型案例：多医院数据共享、制造联盟协同

AGW 的理念和技术框架有望在多个行业中实现落地，尤其在医疗和制造业这两个对数据安全与协作效率要求极高的领域中表现突出。

在医疗行业中，多个医院之间由于政策与伦理限制，无法直接共享患者的原始数据。但在癌症筛查等场景中，往往需要多机构模型协同，进行远程推理和辅助决策。通过将 AGW 部署于医院云边界，实现了加密图像特征的流通与诊断建议的回传，在使医院之间的 Agent 可以像本地一样进

行推理合作的同时，保障患者数据从未离开本院系统。这种模式不仅提高了诊断准确率，也大大减少了传统远程协作中的接口复杂性与合规风险。

在制造业领域中，一个典型的场景是产业链中的主制造商与多级供应商、物流服务商之间的协同调度。传统上，这种合作依赖于固定的数据接口、文件同步或人工协调，效率低且数据不透明。借助AGW，各方部署的Agent可在不暴露关键商业信息（如成本、工艺、存货结构）的前提下，自动交换预测结果、产能评估、发货计划等高阶语义信息。这种以“意图互通”而非“数据互通”为核心的协作模式，大大提升了供应链的响应能力和柔性调度能力。

2.3 To C：个人 Agent 互联与能力延伸

在个人终端场景中，每个用户可以拥有多个本地或云端部署的 AI Agent，如手机助手、智能音箱、车载 AI、AR 眼镜中的实时翻译 Agent、内容整理 Agent、以及个人笔记或任务管理 Agent 等。这些个人 Agent在AI Agent 通信网关的组织协调下，形成一个多Agent的协同网络，实现能力协同、隐私保护与体验统一。

2.3.1 通信隐私保护与去中心化连接

在传统“云-端”架构中，个人 Agent 的能力调用和数据交互通常依赖中心化平台（如大厂服务器）。然而，随着用户对数据主权的重视，以及隐私法规如 GDPR（General Data Protection Regulation，通用数据保护条例）的趋严，新的 Agent 互联模式开始强调“去中心化连接”与“本地数据优先”的原则。在此背景下，AI Agent 通信网关作为一个轻量化、可控的本地中枢节点，承担了 Agent 发现、身份认证、任务调度和通信协议管理等关键职能。

在新的Agent互联模式架构中，所有本地 Agent 首先通过局域内的 P2P 协议（如 mDNS、WebRTC、Bluetooth Mesh）自动完成身份发现与协商，再通过 AI Agent 通信网关注册其能力与接口。用户授权的数据（如联系人、兴趣偏好、行为日志）被优先保存在本地 Agent的数据沙箱中，只有在跨 Agent 协同或跨终端迁移时，网关才通过加密的边缘通道（如零信任模型 + Diffie-Hellman 密钥协商）进行调度和中继，无需接触中心服务器。

另外，去中心化连接还能实现跨平台的 Agent 互联，例如，用户的车载 Agent 在驾驶途中可主动与手机 Agent 进行配对同步日程，当靠近家中 Wi-Fi 时，家庭智能音箱 Agent 即可与其共享状态，实现无缝上下文延续。所有通信均由 AI Agent 通信网关统一协调，并支持用户通过策略配置来控制哪些 Agent 可以互联、互通，以及共享何种能力，从而实现数据自主与控制权归用户。

2.3.2 典型案例：AI助手、内容推荐、个性化搜索

在用户的日常生活中，AI 助手、内容推荐和个性化搜索已成为最常见的智能服务场景。而在 Agent 互联架构的背景下，这些服务不再依赖单一智能体，而是由多个 Agent 协同完成。

在AI助手场景中，当用户向 AI 助手提出“我下周有哪些空闲时间可以安排短途出行？”这一请求时，AI Agent 通信网关将调用日程 Agent、位置感知 Agent、天气预报 Agent 和内容推荐 Agent 进行任务分解：日程 Agent 检索用户行程；位置 Agent 结合用户常驻地和交通习惯提供出行窗口；天气 Agent 预判目的地天气；内容推荐 Agent 基于用户兴趣与历史行为推荐目的地。最终，由 AI 助手 Agent 将结果汇总并通过自然语言反馈给用户。

在个性化搜索场景中，网关根据搜索意图自动编排多个 Agent：本地文件搜索 Agent、知识问答 Agent、订阅信息 Agent（如 RSS/微博）同时参与推理，各自返回结构化结果；融合Agent（Fusion Agent）进行优先级排序和冲突合并，再统一展现。由于所有个人数据处理过程均在网关与本地Agent之间完成，搜索结果更贴合个人语境且不会泄露数据。

在内容推荐场景中，Agent 网络也实现了多源融合与语境适应。例如，在用户沉浸于阅读或观看内容时，媒体推荐 Agent 会结合当前内容主题、历史偏好和时间上下文（如深夜不推荐高能量视频）进行推送；而语言生成 Agent（如写作辅助）则可根据当前任务状态与用户风格，进行短文补全、句式重构或语义延伸等操作。所有推荐行为和模型调优过程均由 AI Agent 通信网关记录并反馈给本地个性建模 Agent，从而实现个体画像的长期演进与动态调优。

通过 AI Agent 通信网关的统一连接、协同与策略化管理，To C 场景中的个人 Agent 网络逐步具备“能力自治”、“数据主权”、“多模态协同”的特点，为用户提供始终如一、隐私可控的智能体验，真正实现了AI 能力在个人生活各个维度的自然延伸与增强。

3 AI Agent 通信网关通信架构

3.1 组网和通信形式

AI Agent 的广泛部署正在重塑未来家庭的智能网络架构。随着机器人、无人机、机器狗、智能家居终端、老年陪护设备和智慧教育助手等多种类型的 AI Agent 纷纷入驻家庭环境，家庭网络已经从传统的“终端接入”模式，演变为以“多 Agent 协同、自治通信与异构融合”为核心的新型架构。这对家庭网络的网关提出了全新的诉求与挑战。如图2所示是家庭场景的 Agent 网络，其中涉及的概念和技术将在子章节中进行描述。

3.1.1 组网形式

AI Agent 通信网关的组网，实质上是组成一张由 AI Agent 通信网关所构成的虚拟网络。该虚拟网络与物理网络一样，可以有其自身的拓扑结构，如星型组网、树形组网、环形组网、Mesh 组网等。除了拓扑结构，一张网络通常还涉及到层级的划分，例如，在 IP 园区网络、IP 城域网等场景中，常常有接入层–汇聚层–骨干/核心层的划分。

3.1.2 通信形式

不论AI Agent通信网关组网的形式如何，最终目的都是为了支撑AI Agent通信网关之间实现高效的信息分发。从信息分发角度，AI Agent通信网关之间的通信可分为以下几类：

直接通信

直接通信是指，发送信息的网关直接指定信息的接收方，可进一步分为以下几种主要模式：

- **点到点：**顾名思义，是指一个网关向另一个网关发送信息，这是最常见的通信模式，例如，IP单播就是这种模式。
- **点到多点：**类似于IP组播，一个网关同时向多个网关直接发送信息。
- **洪泛：**与IGP/BGP协议的洪泛类似，一个网关也可在一定范围内将信息洪泛到全部节点。

间接通信

间接通信是指，发送信息的网关并不直接指定接受的网关，可进一步分为以下几种主要模式：

- **订阅-分发：**发送信息的网关并不知道有哪些网关需要接受信息，它会先将信息发送到一个中心汇聚节点，该汇聚节点根据订阅信息再将信息分发给订阅者。该模式其实可拆解为上述直接通信中“点到点”与“点到多点”的组合，但从应用层一个完整的、端到端的信息发送事件角度而言，订阅-分发是一种非常常用且高效的信息分发方式，适用于多网关相互配合的集群通信场景。

为了支持各种场景下的AI Agent通信，AI Agent通信网关应尽量支持上述各类直接、间接的通信模式。

3.2 AI Agent 通信网关架构

AI Agent通信网关的整体架构分为通信模块、核心管理模块、安全与隐私保护模块、性能优化模块、接口模块和网关互联模块。各模块之间相互协作，共同实现多智能体间高效通信与协作。AI Agent通信网关架构的总体框架如图3所示。

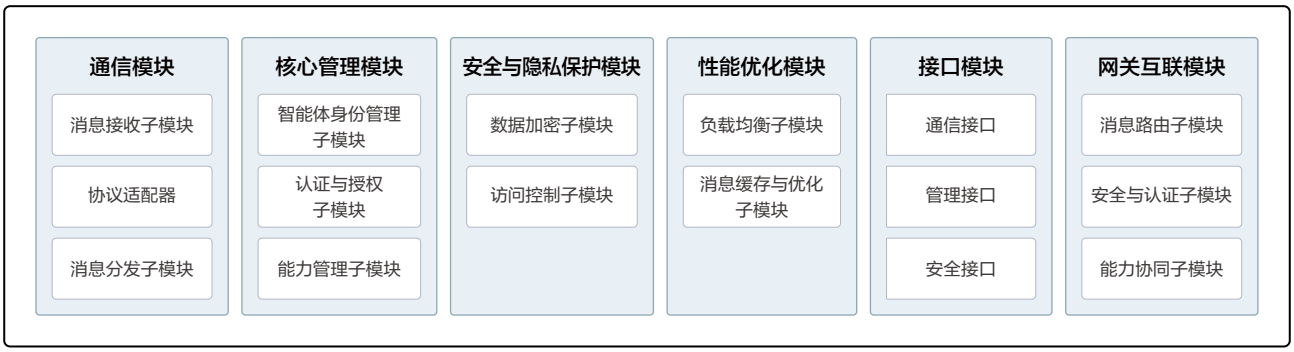


图3　AI Agent 通信网关架构的总体框架

对六大模块的详细介绍如下所述：

通信模块

通信模块是 AI Agent 通信网关与智能体之间交互的前端，负责消息接收、协议适配和分发。它包含以下三个功能子模块：

- **消息接收子模块：**接收来自不同智能体的通信请求，支持请求–响应、发布–订阅、发后即忘和流式传输等多种通信模式。
- **协议适配器：**对不同智能体的通信协议进行转换和适配，确保消息格式统一，便于后续处理。
- **消息分发子模块：**根据目标智能体的地址和通信模式，将消息高效地分发到目标智能体。

核心管理模块

核心管理模块是 AI Agent 通信网关的中枢，负责智能体的身份管理、认证授权以及能力匹配。它包含以下三个功能子模块：

- **智能体身份管理子模块：**通过用户名 & 密码、数字证书、生物识别等方式验证智能体的身份，并根据预设的授权策略，控制智能体对资源的访问权限。
- **认证与授权子模块：**为每个接入的智能体分配唯一的 Agent ID，并存储智能体的身份信 息，包括名称、类型、所属组织等。
- **能力管理子模块：**解析智能体上报的能力描述信息（功能、特性、通信模式等），存储在智能体目录中供其他智能体查询，并根据任务需求动态发现具有相应能力的智能体，建立通信连接。

安全与隐私保护模块

安全与隐私保护模块是 AI Agent 通信网关的重要组成部分，确保通信数据的安全性和智能体的隐私。它包含两个功能模块：

- **数据加密子模块：**支持多种加密算法（如AES、RSA），对通信数据进行加密，并生成、分发和管理加密密钥。
- **访问控制子模块：**定义智能体对资源的访问权限，限制智能体对其他智能体隐私信息的访问，确保数据仅在授权范围内共享。

性能优化模块

性能优化模块通过多种手段提升 AI Agent 通信网关系统的整体性能和稳定性。它包含两个功能子模块：

- **负载均衡子模块：**实时监测智能体的负载情况和系统资源的使用情况，根据负载情况合理分配通信请求，避免某些智能体过载。
- **消息缓存与优化子模块：**缓存频繁发送的消息，减少重复计算和传输，同时优化消息的格式和传输路径，提高通信效率。

接口模块

接口模块为智能体提供标准化的接口，方便其接入和交互。它包含以下三个接口：

- **通信接口：**提供统一的通信接口，支持多种通信模式和协议。
- **管理接口：**用于智能体的身份注册、能力描述上传、查询智能体目录等功能。

网关互联模块

网关互联模块负责实现不同 AI Agent 通信网关之间的高效协作，支持更大范围的智能体协同和资源共享。它包含以下三个功能子模块：

- **消息路由子模块：**实现跨网关的消息转发，根据目标智能体的 Agent ID 或任务需求动态选择最佳路径，同时考虑负载均衡与优化。
- **安全与认证子模块：**通过身份认证和数据加密机制，确保网关之间通信的安全性。
- **能力协同子模块：**支持网关之间的能力发现与资源共享，实现复杂任务的协同处理。

3.3 核心技术要素

3.3.1 Agent ID：全局唯一的数字身份体系

AI Agent接入网络之后，需要一个唯一的数字身份——Agent ID来标识该AI Agent。在家庭内、云内、企业网内部，作为AI Agent身份标识的Agent ID必须唯一，避免与其他AI Agent冲突，以保证Agent被唯一地、正确地索引和访问到。无论是数字Agent还是物理Agent，无论是通过固网、Wi-Fi或Internet接入，还是通过3GPP蜂窝网络接入，AI Agent都需要获得一个唯一的数字身份标识，智能体间通信时基于该数字身份标识进行安全认证和行为授权，以确保用户的隐私安全。

在这种情况下，就需要建立一个AI Agent数字身份管理体系，对Agent ID进行统一地分配和管理，以确保各个组织、区域能够为新入网的AI Agent高效地分配数字身份标识，并保证该标识全局唯一、不冲突。

3.3.2 Agent DNS：基于数字身份的注册、查找、寻址机制

AI Agent互联协作时，需要能够根据Agent的名称或者ID正确找到Agent的URL地址，并根据Agent的URL地址对Agent进行访问。因此，AI Agent通信网关协议需要支持提供类似Internet的DNS服务，如图4所示，Agent DNS服务需要包括以下几个方面：

- 支持对新加入的Agent完成注册。
- 支持对已注册的Agent查找机制。
- 支持对已注册的Agent更新机制。
- 支持对已注册的Agent退出机制。

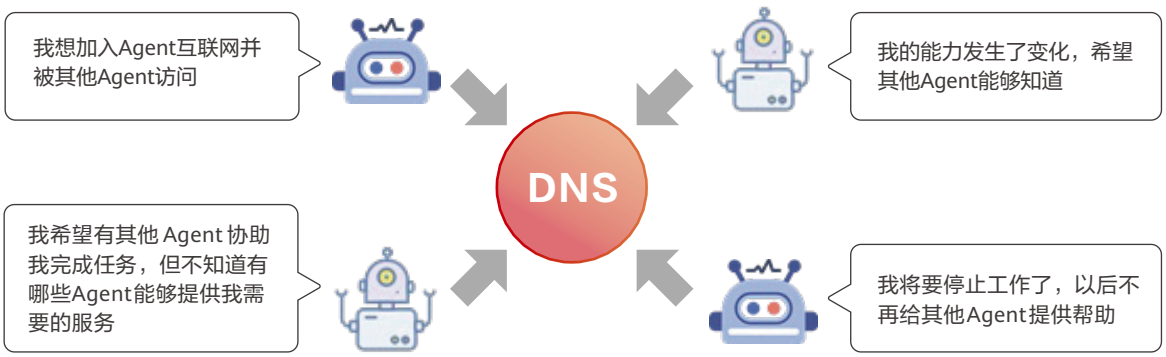


图4　Agent DNS服务

3.3.3 Agent 路由：基于数字身份或能力的寻址机制

由于AI Agent会进行云内访问、跨云访问、端云访问、边云访问等操作，AI Agent通信网关需要支持Agent路由，即基于Agent数字身份的寻址机制。当Agent需要与其他Agent进行任务协作时，会将协作Agent的数字身份和协作请求发送给Agent通信网关，Agent通信网关能够基于Agent寻址功能将协作请求准确地发送给协作Agent。Agent寻址功能可能会存在以下两种模式：

- 基于Agent数字身份的寻址模式：如图5所示，当Agent只知道协作Agent的数字身份、不知道协作Agent的访问方式时，Agent通信网关将基于数字身份的Agent路由，将协作请求准确地发送给协作Agent 。

图5　基于Agent数字身份的寻址模式

- 基于Agent能力的寻址模式：当Agent只知道协作任务请求、不知道协作Agent的数字身份时，Agent通信网关将基于协作任务请求，从经过合法认证的Agent中选择能力最为匹配的Agent作为协作Agent，将协作请求发送给协作Agent 。

3.3.4 Agent 能力描述标准及能力评估体系

理解自然语言是AI Agent的显著特征之一，Agent能够读懂其他Agent的能力是Agent实现相互协作的基础。Agent的能力一般都通过自然语言来描述，因此需要建立一套Agent能力描述标准，将具备不同能力的Agent明确地区分开来，保证Agent在协作时能够准确地找到能力符合要求的Agent。

同时，还需要建立一套Agent能力评估体系，对Agent的能力进行客户评价、打分，使得能力强、表现优异的Agent能够脱颖而出，得到更多的访问和使用机会；而能力差的Agent能够逐渐退出Agent互联网，实现Agent间的良性竞争和能力进化。

3.3.5 与传统IP网络的兼容设计（数字身份-IP地址映射）

Agent互联网是建立在传统互联网、云网络之上的一张新型互联网，能够实现人-Agent、Agent-Agent、Agent-Internet之间的互访。因此，Agent互联网需要兼容传统的IP网络。

Agent接入Agent互联网的第一步是接入传统互联网，拥有一个IP地址，确保URL合法且可被访问；第二步是向Agent数字身份管理机构申请一个合法唯一的Agent ID，并将数字身份Agent ID和IP地址进行映射，将Agent名称、Agent ID、URL、Agent能力描述等信息发布出去。对目标Agent进行访问时，先实现对目标Agent所在URL或IP地址的访问，找到传统互联网的接入实体，再通过Agent数字身份，实现对目标Agent的访问。

3.3.6 安全机制与合规治理

Agent认证与授权

Agent需要严格的认证与授权机制，防止恶意Agent装成合法Agent，发起数据窃取、干扰网络运行、频繁访问等攻击行为。Agent认证不仅包括合法性认证和安全性认证，还需要包括能力认证。不合法、不安全、能力描述不符合标准的Agent能接入Agent互联网。

用户对特定数据的访问可以通过用户身份进行授权，Agent对特定资源数据的访问也需要基于Agent ID进行授权。同一个Agent执行不同的任务时，所拥有的权限也可能不同，因此，Agent通信网关协议需要支持在不同Agent执行不同任务的场景中进行差异化授权，防止出现由于Agent越权访问导致网络拓扑信息、用户隐私数据、设备配置参数等信息发生泄露。

通信计费与追溯

Agent对外可以提供免费或者计费服务，用户访问Agent、Agent访问Agent都需要一套完善的计费体系，Agent提供商可以根据访问流量或者访问次数对访问者收费。Agent通信网关协议架构需要支持Agent的访问历史追溯能力，方便Agent提供商对外计费和对Agent提供商追责。

4 标准化展望与未来路线图

4.1 关键标准方向

4.1.1 AI Agent 终端与网关协同

AI Agent 由于智能化程度高，其通信模式和通信需求可能更加灵活多变。同一个终端，在不同的时间，可能有完全不同的流量模型和安全需求。通过引入 Agent 终端与网关的协议，可以实现网络根据 Agent 终端当前的需求，实时生成相应的网络策略、划分相应的网络资源，以保障终端通信的服务质量和安全保护。

4.1.2 AI Agent 通信网关间通信

如前文所述，通过引入 AI Agent 通信网关组成网关虚拟网络，并基于此对 Agent 之间的通信进行支撑，可以极大地改善 Agent 之间通信的可扩展性、安全保障以及质量保障。因此，AI Agent 通信网关之间的组网和通信协议将会是必须项。通过标准化，不同厂商的 Agent 通信网关可以实现互通，建立开放的生态，真正使 Agent 之间的通信受益。

4.1.3 AI Agent终端准入控制

AI Agent终端是指硬件终端形态的Agent，这与当前较受关注的基于软件形态的、面向Internet用户提供服务的Agent有所不同。从网络终端的角度看，其第一步是需要便捷、安全地接入网络；网络则需要根据终端的类型、厂商、功能、ID等信息进行准入控制，防止非法Agent接入用户网络，造成信息泄露、病毒或非法信息扩散等安全风险。

AI Agent终端的准入控制协议可参考当前已有的IoT（Internet of Things，物联网）领域终端接入的架构和协议，除此以外，应在IoT的基础上，针对Agent终端智能化、自主性程度高的特点，考虑增加对Agent终端进行基于角色、业务属性信息、行为记录等更高维度的访问控制。这些在语义层面都需要新的扩展。

4.2 产业合作建议与标准组织协同路径

4.2.1 建立开放的厂商生态

通过构建AI Agent终端-AI Agent通信网关、AI Agent通信网关之间的标准化协议，可以实现多厂商设备之间的互通，建立繁荣的生态。

4.2.2 构建全球范围的AI Agent通信网关网络

除了多厂商间的互通，AI Agent通信网关还应做到全球可达。将全球可达的IP网络作为Underlay是一个不二选择，通过运营商、云厂商间的协作，将AI Agent通信网关的网络平面有效地运维起来。

4.2.3 多标准组织协同

IETF、3GPP、ITU-T、ETSI等国际标准组织应在该议题上保持密切联络，互为输入、输出，制定出能有效支撑实际业务需求的标准技术。

参考文献

[1] Anthropic. Building Effective AI Agents. [Online] Available: https://www.anthropic.com/engineering/building-effective-agents

[2] Gartner. Gartner Identifies the Top 10 Strategic Technology Trends for 2025. [Online] Available: https://www.gartner.com/en/newsroom/press-releases/2024-10-21-gartner-identifies-the-top-10-strategic-technology-trends-for-2025

[3] Outshift. Outshift | Internet of Agents. [Online] Available: https://outshift.cisco.com/the-internet-of-agents