RTGWG
Internet-Draft
Intended status: Informational
Expires: 28 May 2026

Z. Han, Ed.
Z. Ruan, Ed.
R. Pang
M. Han
China Unicom

24 November 2025

# Agent Gateway Intercommunication Framework
draft-han-rtgwg-agent-gateway-intercomm-framework-00

## Abstract

This document defines the framework and requirements for intercommunication between Agent Gateways (AGw) in the Agent Internet (IoA) ecosystem. It specifies a hierarchical layered model, functional components, protocol requirements and deployment consideration for AGw interconnection. The framework aims to address data synchronization, protocol compatibility, and security challenges in cross-domain agent collaboration, enabling efficient and scalable communication for distributed intelligent agents.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 28 May 2026.

## Copyright Notice

Table of Contents



## 1. Introduction

The Agent Internet (IoA) enables collaborative work among massive numbers of AI agents deployed across diverse environments. As the core network component in IoA, Agent Gateway (AGw) acts as a "connection hub" and "security steward" that bridges intra-domain agents and cross-domain networks. It handles agent registration, discovery, protocol translation, and security protection.

In distributed IoA ecosystems, numerous agents collaboration relies heavily on intercommunication between AGws. For example, an agent in a smart park may need to collaborate with a cloud-based payment agent, requiring their respective AGws to exchange capability information, network status, and task context. However, existing network communication mechanisms lack standardized frameworks for AGw interconnection, leading to challenges such as inconsistent data synchronization, incompatible protocols, and inadequate network quality awareness.

This document specifies the Agent Gateway Intercommunication Framework to address these challenges. It defines the architectural patterns for AGw intercommunication, core content to be transmitted, protocol requirements, and target scenarios. This framework builds on existing IoA components such as Agent Certificate Authority (ACA) and Agent Registration Server (ARS) [I-D.zl-agents-networking-framework], ensuring compatibility with existing agent networking architectures while enabling secure, efficient, and scalable cross-domain AGw collaboration.

## 2. Conventions Used in This Document

### 2.1. Abbreviations

### 2.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 3. Terminology

AGw (Agent Gateway): A network component that acts as a connection hub and security steward for agent communication, responsible for route management, protocol translation, security protection, and traffic control.

AGw Intercommunication: The process of data exchange and collaborative operations between AGws deployed in different domains (e.g., different parks, enterprises, or network segments).

Agent Metadata: Core information about intelligent agents, including identity identifier, capabilities, endpoint address, status, and supported protocols.

Network Quality Metrics: Key indicators reflecting cross-AGw communication performance, including latency, packet loss rate, bandwidth, and jitter.

Protocol Translation: The function of converting between different communication protocols (e.g., HTTP, MQTT, gRPC) and data formats (e.g., JSON, Protobuf) to ensure interoperability.

Cross-Domain Collaboration: Collaborative task execution between agents located in different network domains, facilitated by AGw intercommunication.

## 4. Motivation

With the proliferation of intelligent agents in various industries, cross-domain collaboration has become a key requirement for IoA. AGw intercommunication is critical to enabling this collaboration, but current implementations face several challenges as below. To address these challenges, this framework defines standardized intercommunication mechanisms that ensure consistent data synchronization, network quality awareness, protocol compatibility, security, and scalability for AGws in distributed IoA ecosystems.

### 4.1. Inconsistent Data Synchronization

Lack of standardized agent metadata exchange formats leads to incomplete or outdated information sharing between AGws, preventing accurate agent discovery.

### 4.2. Network Quality Blindness

AGws lack mechanisms to exchange real-time network quality metrics, resulting in agents collaborating over suboptimal paths with high latency or packet loss.

### 4.3. Protocol Incompatibility

Different AGws may adopt diverse communication protocols, causing interconnection failures and hindering cross-domain agent interactions.

### 4.4. Security Risks

Cross-domain AGw communication involves sensitive agent identity and task data, requiring robust authentication and encryption mechanisms that are currently lacking.

### 4.5. Scalability Limitations

Existing point-to-point communication models cannot efficiently support large-scale AGw deployments (e.g., hundreds of park AGws), leading to performance bottlenecks.

## 5. AGw Intercommunication Framework

The AGw intercommunication framework is structured into four hierarchical layers. This enables AGws to function both as communication gateways with advanced networking capabilities and as AI agents that optimize agents communication and collaboration.

### 5.1. Application Service Layer

Serves as the "intelligent directory" for the agent ecosystem, providing agent registration, capability discovery, identity management, and semantic matching between business requirements and agent capabilities.

Interconnection Role: AGws exchange agent metadata including capabilities, security levels, response times, and service SLAs through application-layer protocols, maintaining a distributed directory of available agents across domains.

### 5.2. Orchestration & Control Layer

Provides centralized intelligence for complex task decomposition, policy enforcement, path orchestration, and global governance of cross-domain agent collaborations.

Interconnection Role: Analyzes complex task requirements and selects optimal agent combinations and network paths based on comprehensive factors including security policies, service levels, and network conditions.

### 5.3. Agent Connectivity Layer

Acts as the "communication bridge" between heterogeneous agents, providing protocol translation, semantic adaptation, and abstraction of underlying network capabilities.

Interconnection Role: Enables seamless communication between agents with different technical implementations by performing real-time protocol conversion and semantic mediation, while abstracting complex network functions into simplified, agent-accessible services.

### 5.4. Network Communication Layer

Provides the foundational connectivity with guaranteed quality of service, differentiated SLA enforcement, and reliable data transmission between AGws.

Interconnection Role: Establishes and maintains high-quality communication channels between AGws, continuously monitoring network metrics (latency, loss, bandwidth) to ensure SLA compliance for agent collaborations.

## 6. AGw Functional Components

### 6.1. Application Service Layer Components

* Agent Registry: Maintains a database of registered agents with their capabilities, security levels, and service attributes, synchronizing this information with peer AGws.

* Capability Discovery: Processes semantic queries to match business requirements with appropriate agent capabilities across domains.

* Identity Manager: Verifies agent identities through ACA integration and manages authentication credentials for cross-domain access.

### 6.2. Orchestration & Control Layer Components

* Task Decomposer: Breaks down complex tasks into executable subtasks and identifies required agent capabilities for each step.

* Path Orchestrator: Computes optimal agent combinations and network paths based on security, service SLA, and network SLA requirements.

* Policy Controller: Enforces governance policies, security rules, and compliance requirements across all cross-domain collaborations. Acts as the "communication bridge" between heterogeneous agents, providing protocol translation, semantic adaptation, and abstraction of underlying network capabilities.

### 6.3. Agent Connectivity Layer Components

* Protocol Translator: Converts between different agent communication protocols and data formats in real-time.

* Semantic Adapter: Ensures semantic compatibility between agents with different data models and interaction patterns.

* Service Abstractor: Presents network capabilities as callable services that agents can utilize through simplified APIs.

### 6.4. Network Communication Layer Components

* QoS Enforcer: Implements traffic prioritization, bandwidth allocation, and latency management for different classes of agent traffic.

* SLA Monitor: Continuously measures network performance metrics and triggers alerts when SLAs are violated.

* Secure Manager: Establishes and maintains encrypted tunnels between AGws with mutual authentication.

## 7. AGw Intercommunication Requirements

* Agent Identity Identification & Discovery: Distinguish agents from real users, integrate semantic understanding and addressing to match business needs with corresponding agents.

* Heterogeneous Compatibility: Different agents vary in resources and supported protocols, so adaptation and protocol conversion are required for agents communication.

* Efficient Agent Communication: For agent interaction, consider network reachability, QoS guarantee, and differentiated SLA services. Due to high pressure in peer-to-peer collaboration among multiple agents, convergence is needed to enable hierarchical communication.

* Agent Scheduling & Management: Realize agent scheduling within and across enterprise campus; unify orchestration of network resources and agent services to align network and business.

* Security & Privacy: Implement access management and permission control to enhance security.

## 8. Deployment Considerations

* Hierarchical Deployment: For large enterprises or service providers, AGws should be deployed at domain edges (e.g., campus gateways, cloud VPCs), with regional directory servers at network aggregation points.

* Redundancy Design: Critical domains SHOULD deploy redundant AGws to avoid single points of failure. Directory services SHOULD be deployed in a clustered mode for high availability.

* Network Integration: AGws SHOULD be integrated with existing network infrastructure (e.g., SDN controllers) and IoA components (ACA, ARS) via standard APIs to enable unified orchestration of network and agent resources.

* Extensibility: The intercommunication protocols and data formats SHOULD be designed with extensibility in mind, using versioning and optional fields to accommodate future enhancements without breaking backward compatibility.

## 9. Security Considerations

This document does not have any specific security considerations.

## 10. IANA Considerations

This document does not have any IANA considerations.

## 11. References

### 11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

### 11.2. Informative References

[I-D.zl-agents-networking-framework] Zhang, L., Liu, B., Geng, N., Shang, X., Gao, Q., and Z. Li, "Agents Networking Framework for Enterprise and Broadband", Work in Progress, Internet-Draft, draft-zl-agents-networking-framework-00, 2 November 2025, <https://datatracker.ietf.org/doc/html/draft-zl-agents-networking-framework-00>.

[I-D.liu-rtgwg-agent-gateway-requirements] Liu, B., Geng, N., Shang, X., Gao, Q., and Z. Li, "Requirements for Agent Gateway", Work in Progress, Internet-Draft, draft-liu-rtgwg-agent-gateway-requirements-00, 2 November 2025, <https://datatracker.ietf.org/doc/html/draft-liu-rtgwg-agent-gateway-requirements-00>.

[I-D.mzsg-rtgwg-agent-cross-device-comm-framework]
Mao, J., Zeng, G., Liu, B., Geng, N., Shang, X., Gao, Q., and Z. Li, "Cross-device Communication Framework for AI Agents in Network Devices", Work in Progress, Internet-Draft, draft-mzsg-rtgwg-agent-cross-device-comm-framework-01, 1 November 2025, <https://datatracker.ietf.org/doc/html/draft-mzsg-rtgwg-agent-cross-device-comm-framework-01>.

[I-D.zeng-mcp-network-measurement]
Zeng, G. and J. Mao, "MCP-based Network Measurement Framework: Using Model Context Protocol for Intelligent Network Measurement", Work in Progress, Internet-Draft, draft-zeng-mcp-network-measurement-00, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-zeng-mcp-network-measurement-00>.

## Acknowledgements

TBD.

## Contributors

TBD.

## Authors' Addresses

Zhengxin Han (editor)
China Unicom
Beijing
China
Email: hanzx21@chinaunicom.cn

Zheng Ruan (editor)
China Unicom
Beijing
China
Email: ruanz6@chinaunicom.cn

Ran Pang
China Unicom
Beijing
China
Email: pangran@chinaunicom.cn

Mengyao Han
China Unicom
Beijing
China
Email: hanmy12@chinaunicom.cn