nmop
Internet-Draft
Intended status: Standards Track
Expires: 29 July 2026

Y. Fu
Q. Sun
X. Song
C. Xie
China Telecom

25 January 2026

Agent Communication Framework for Network AIOps
draft-fu-nmop-agent-communication-framework-00

Abstract

As the development of large model and agent technology, it is a trend for multi-agent collaboration to solve complex problems. This document proposes an Agent Communication Framework, a multi-agent communication and collaboration framework that facilitates the coordination of heterogeneous multi-agents and supports intelligent network operations and maintenance (AIOps). Its architecture includes an AI gateway and an Agent Name Service, along with capabilities such as monitoring and tracking, as well as security protection. Agent Communication Framework provides a comprehensive solution for multi-agent communication and collaboration, laying the foundation for future interactive, scalable, secure, and controllable multi-agent network intelligent operations and maintenance.

Table of Contents

1. Introduction

As the rapid development of AI technology, network operations and maintenance have evolved from efficiency improvement to automation, through the Data-Driven Digital age with the rise of AIOps (intelligent network operations and maintenance), now striding towards the Agentic AI stage. In this new phase, the collaborative capabilities of intelligent agents will drive operations and maintenance toward a higher level of autonomy. However, current multi-agent collaboration still lacks reliable mechanisms for agent addressing, communication, and orchestration scheduling. It introduces several requirements as below:

Agent registering and discovering : With the rapid developments of multi-agent collaborative scenarios, traditional service discovery mechanisms face several challenges. They are unable to adapt to the multi-heterogeneous and dynamically changing capability of agents. There is a lack of a unified capability of registration and discovery framework for the cross-domain and spans different subject agents,

result in low efficiency of task-driven precise collaboration. There is an urgent need to build a global agent capability registration mechanism, dynamically maintain the real-time capability database of agents across the network, and generate optimal matching strategies based on task requirements.

Cross-domain interconnection: In some task-oriented collaboration scenarios, it may encounter interoperability challenges—both within intra-domain and inter-domain use cases. In inter-domain scenario, agents belonging to different domains must discover, access, and securely interact with one another to enable effective collaboration.

Security Operations: To support large-scale deployment of intelligent agents, a comprehensive operation-level security framework is required that integrates management, access control, traceability, and authentication tailored for agent-centric environments., with security mechanisms and capabilities such as zero trust, communication encryption and decryption, and supervision embedded in the protocol.

1.1. 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.

1.2. Definition and Terminology

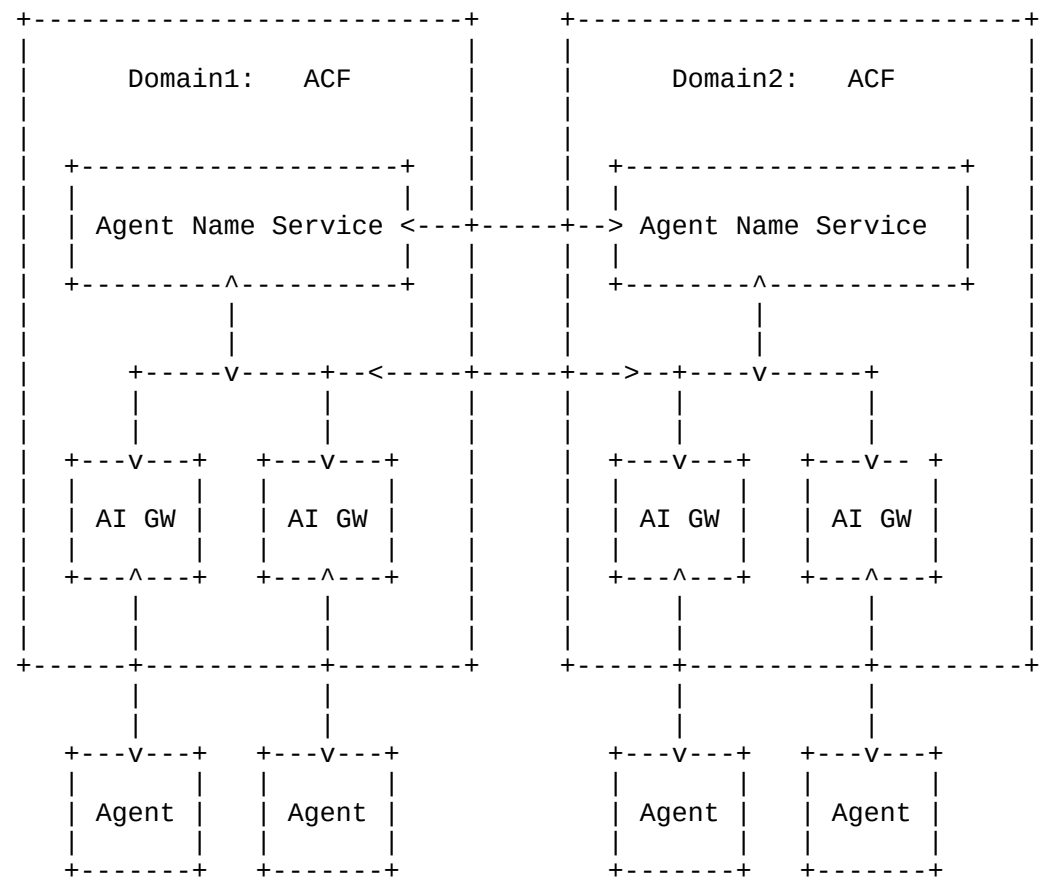
ACF：Agent Communication Framework

ANS：Agent Name Service

AI Gateway：AI GW

2. Agent Communication Framework and Components

To address the requirements described above, we propose an Agent Communication Framework for intra-domain and inter-domain agent communications. It consists of two components: AI Gateway and Agent Name Service (ANS). It is the “Connection and control Hub” for agent communication. The overview of the agent communication framework is shown in Figure 1.



As described in Section 1, efficient interconnection among agents relies on clear identity information and capability-based discovery. Therefore, a unified identity identification and agent information management mechanism forms the foundation for the secure agent interconnection. Agent Communication Framework issue unique identity IDs for each agent and establish an authentication framework to ensure the security of mutual visits. They are capable of managing information for a massive number of agents, able to obtain agent information through multiple methods to ensure information comprehensiveness. In Agent Communication Framework, a semantics-based dynamic agent addressing scheme is proposed to enhance the accuracy and flexibility of agent interconnection and collaboration, enabling interoperability across different domains. In Intra-domain scenarios, the agent communication framework enables the discovery and management within the domain and presents a unified proxy externally. Independent AI gateways realize the unified access and mutual discovery of agents within domains such as edge homes and the

Internet of Things. In inter-domain scenarios, information synchronization mechanism needs to be done by designing as an agent information repository in Agent Name Service (ANS) between different domains, combining with the existing DNS mechanisms for cross-domain addressing and discovery of agents.

2.1. AI Gateway

An AI Gateway is a reliable, efficient, and secure interconnection hub for agents. The main functions of AI Gateway include:

* Service Proxy: Service Proxy function acts as an intelligent network address translation (NAT) layer that seamlessly translates between internal and external network addresses, enabling secure communication between private services and external clients. By masking the identities and IP addresses of internal agents or services, it effectively hides the internal network topology from external access, thereby enhancing security, reducing exposure to potential threats, and simplifying service exposure management.

* Traffic forwarding and optimization: The AI Gateway provides intelligent traffic forwarding and optimization capabilities, including Quality of Service (QoS) guarantees to prioritize critical workloads, dynamic multi-channel selection for optimal path routing based on real-time network conditions, and packet compression to reduce bandwidth consumption and latency. Additionally, it leverages AI-driven analytics to adaptively manage traffic flows, ensure reliable delivery, and enhance overall network efficiency and user experience.

* Security protection: It provides comprehensive security protection by implementing end-to-end channel encryption to ensure data confidentiality and integrity during transmission, coupled with advanced traffic security detection and real-time threat mitigation mechanisms— such as anomaly detection, intrusion prevention, and malicious payload filtering— to safeguard against cyberattacks and unauthorized access.

* Monitoring and auditing: It provides comprehensive monitoring and auditing capabilities by continuously observing and logging all interaction behaviors between agents, including request sources, destinations, timestamps, data payloads (where permitted), and access patterns.

In addition to the capabilities described above, the AI Gateway also supports the requirements of high concurrency, high reliability, as well as scalability.

* The AI Gateway supports persistent, always online sessions for heterogeneous agents, enabling seamless dynamic participation— where agents can join or leave a session at any time without disrupting the workflow. It ensures session continuity through intelligent checkpointing and resumption mechanisms, allowing tasks to resume exactly from the point of interruption in the event of network disconnections or agent failures, without requiring the entire task to be restarted. This capability maintains task integrity, improves resource efficiency, and enhances reliability in complex, multi-agent collaborative scenarios.

* The AI Gateway is designed to deliver highly concurrent, secure, and ultra-low-latency asynchronous communication for multi-agent systems, supporting scalable workloads with millions of simultaneous connections. It ensures robust security through end-to-end encryption and fine-grained access control, while optimizing message routing and processing to minimize latency— enabling efficient, real-time coordination among large-scale heterogeneous agents

* The AI Gateway is designed for high scalability, supporting both horizontal and vertical expansion to accommodate growing multi-agent workloads. Horizontally, it enables elastic scaling of gateways to handle increased traffic and agent density by dynamically adding or removing nodes based on demand. Vertically, it implements recursive addressing across hierarchical gateway layers, allowing seamless inter-layer communication and efficient routing in large-scale, nested, or federated agent architectures. Together, these capabilities ensure the system can scale flexibly and efficiently— both outward across distributed deployments and upward through logical abstraction layers— while maintaining performance, consistency, and manageability.

* The AI Gateway supports high-reliability requirements for fully autonomous, human-intervention-free interactions among agents. It ensures continuously stable and fault-resilient network connectivity through redundant pathways, automatic failover mechanism— thereby preventing communication disruptions that could otherwise trigger cascading failures across the agent ecosystem. This reliability is critical to maintaining uninterrupted task execution and system-wide stability in mission-critical multi-agent environments.

2.2. Agent Name Service

Agent Name Service provides access and semantic addressing function for multi-agents, and combines with the AI Gateway to provide security protection and monitoring capabilities.

2.2.1. Agent Accessing

* Registration: The Agent Name Service (ANS) provides a secure and structured access mechanism for intelligent agents through an integrated registration and identity management mechanism. It begins with the Registration Module, which receives registration requests from agents, validates their legitimacy (e.g., through credentials, tokens, or domain policies), and initiates the enrollment process. The Security Module then handles cryptographic identity provisioning by accepting the agent's Certificate Signing Request (CSR), verifying its authenticity, and issuing a signed certificate to establish trusted identity. Finally, the Registry securely stores each agent's metadata—including its unique identifier, certificate, capabilities—enabling reliable discovery, authentication, and secure communication across the multi-agents. This end-to-end workflow ensures that only authorized agents are admitted into the system, with verifiable identities and consistent governance.

* Update, Renewal and Revocation: The Agent Name Service (ANS) supports comprehensive lifecycle management for registered agents through secure and auditable update, renewal, and revocation operations. For updates, agents may submit requests to modify their metadata—such as capabilities, protocols, or agent Card information. The ANS server performs signature verification to authenticate the request and ensures backward compatibility; if the changes introduce incompatibilities, the agent must update its version number and do re-registration. Upon successful validation, the ANS updates the corresponding versioned record in its registry. For certificate renewal, agents initiate a renewal request before their current certificate expires. The ANS validates the agent's identity via cryptographic signature verification. After confirmation, it issues a new signed certificate while updating the associated agent entry—ensuring uninterrupted, trusted operation without service disruption. For revocation, agents or administrators can request certificate invalidation in cases of key expiration. After verifying the authenticity of the revocation request through signature checks, the ANS permanently removes the agent's certificate and associated metadata from the registry, immediately terminating its ability to access. All operations are executed under strict cryptographic validation and audit logging, ensuring integrity, traceability, and continuous security across the agent lifecycle.

2.2.2. Agent Addressing

The Agent Name Service (ANS) provides a millisecond-level Semantic Addressing Query capability that enables agent discovery—allowing users or systems to express intent in plain language (e.g., "Poor mobile signal and unstable broadband at home") and automatically resolving it to the most relevant agents (e.g., Home Broadband Agent and Wireless Network Optimization Agent). Semantic-based addressing and discovery of agents requires the Agent Name Service (ANS) to possess comprehensive, detailed descriptive information for all agents. This functionality is implemented through three coordinated components:

The Resolution Module receives semantic resolution requests from agents and leverages RAG techniques to interpret the query and match it to appropriate agent. The Registry then retrieves the corresponding agent's metadata—including its capabilities, protocol details, and certificate—based on the resolved semantic intent. Finally, the Security Module cryptographically signs the retrieved agent information and certificate using the private key, ensuring authenticity and integrity before returning the signed response to the requester.

2.2.3. Security Protection

The Agent Name Service (ANS) incorporates robust security and governance mechanisms to ensure safe and controlled agent interactions. It enforces fine-grained permission control at the agent level through a structured workflow that includes registration requests, administrative approval, and explicit authorization—ensuring that only vetted agents gain access to specific capabilities or resources.

To counter adversarial inputs, ANS integrates prompt injection prevention by inspecting all incoming instructions or queries for malicious patterns, obfuscated commands, or attempts to hijack agent behavior, thereby safeguarding the integrity of agent operations.

Additionally, it implements tiered content security protection to prevent sensitive information leakage, applying data classification policies, context-aware filtering, and output sanitization based on sensitivity levels.

2.2.4. Capabilities Monitoring and Management

The Agent Name Service (ANS) enables real-time monitoring of agent reference, dynamically constructs a graph of agent relationships to visualize interaction patterns and dependencies across the domain, and supports proactive intervention in anomalous or unauthorized behaviors.

The Agent Name Service (ANS) provides intelligent agent capability management by systematically evaluating and verifying the functional competencies, performance characteristics, and operational boundaries of registered agents. This includes assessing declared capabilities, validating actual behavior through runtime evidence or sandboxed testing, and maintaining a trusted, up-to-date profile of each agent's verified skills. By ensuring that advertised capabilities accurately reflect real-world functionality, ANS enables reliable agent discovery, safe composition, and context-aware orchestration within dynamic multi-agent domains.

2.2.5. Cross-domain synchronization

The Agent Name Service (ANS) enables cross-domain collaboration among intelligent agents by securely synchronizing agent information. In inter-domain scenarios, information synchronization mechanism needs to be done by designing as an agent information repository in ANS between different domains, and combining with the existing DNS mechanisms for cross-domain addressing and discovery of agents.

3. Use Case

* Case 1: Home Broadband Service Installation

In the scenario of handling home broadband service installation, we employ a collaborative system comprising 13 agents, including the Intent Recognition Agent, Domain-Specific Configuration Agent, Master Control Agent, Service Validation Agent etc.

Phase 1: Service intent recognition

Agent Used: Intent Recognition Agent; Master Control Agent of service installation

Action: 1.Identify users' service installation requirements by the Intention Recognition Agent. 2.Automatically send the structured service intent to the Master Control Agent.

Phase 2: Service Orchestration and Resource Allocation

Agent Used: Master Control Agent of service installation; Service Orchestration and Resource Allocation Agent

Action: 1.The Master Control Agent sends the service installation request to the Service Orchestration and Resource Allocation Agent, completes the planning of the service path and the evaluation and allocation of resources. 2.The Service Orchestration and Resource Allocation Agent feedback the service path and resource allocation plan back to the Master Control Agent.

Phase 3: Data Preparation and Distribution

Agent Used: Master Control Agent of service installation; Domain-Specific Configuration Agent

Action: 1.The Service installation Master Control Agent initiates data preparation and configuration requests based on the plan. 2.The Domain-Specific Configuration Agent generates the systems corresponding configuration data and completes the automatic configuration of network elements (NEs) / network management systems. 3.As the completion of the configuration, the results are automatically back to the Master Control Agent.

Phase 4: Service Validation

Agent Used: Master Control Agent of service installation; Domain-Specific Configuration Agent; Service Validation Agent

Action: 1.The Master Control Agent triggers the automated service validation process. 2.The Service Validation Agent collaborates with the Domain-Specific Configuration Agent to query the data of configuration and status, and subsequently performs installation verification and validation. 3.The validation results are back to the Master Control Agent, forming a closed-loop validation cycle.

Phase 5: Quality monitoring

Agent Used: Installation and Maintenance Scheduling Agent

Action: 1.The Installation and Maintenance Scheduling Agent performs continuous monitoring of customer services to ensure the quality of new installations.

Phase 6: Customer feedback survey

Agent Used: Personal Intelligent Assistant Agent

Action: 1.The Personal Intelligent Assistant Agent schedules the installation/maintenance engineers for service follow-up and review.

* Case 2: Home Broadband Network Fault Diagnosis

In the scenario of handling home broadband network fault diagnosis, we employ a collaborative system comprising 13 agents, including the Intent Recognition Agent, Preprocessing Agent, Single-Domain Root Cause Analysis Agent, Knowledge Q&A Agent, Fault Handling Agent etc.

Phase 1: User Complaint Intent Recognition and Data Sensing

Agent Used: Intent Recognition Agent; Preprocessing Agent

Action: 1.Identify the type of user complaint by the Intention Recognition Agent. 2.Automatically trigger the data preprocessing function of the Preprocessing Agent based on the complaint type to collect key information such as user devices, alarms, and networks information. 3.Complete unified perception and aggregation of user-side data.

Phase 2: Home Broadband Fault Complaint Handling

Agent Used: MSingle-Domain Root Cause Analysis Agent; Perception Data Collection Agent; Knowledge Q&A Agent; Data Collection Agent

Action: 1.The Single-Domain Root Cause Analysis Agent performs initial root cause analysis based on existing data.
2.If information is insufficient, it triggers the data recollection

mechanism of the Perception Data Collection Agent. The Knowledge Q&A Agent guides the user to supplement key information. The Data Collection Agent complements the missing data. 3. After multiple iterations, it outputs a most likely root cause, impact scope, and recommendations.

Phase 3: Trouble Shooting

Agent Used: Fault Handling Agent; Installation and Maintenance Scheduling Agent

Action: 1.The Fault Handling Agent supports automatic fault recovery. 2.If automatic repair fails, it triggers the Installation and Maintenance Scheduling Agent to generate the optimal dispatch plan based on the location and skills of the installation and maintenance engineers, as well as the urgency of the fault.

Phase 4: Service Validation

Agent Used: End-to-End Testing Agent

Action: 1.The End-to-End Testing Agent initiates tests to ensure service consistency.

Phase 5: Quality monitoring

Agent Used: Installation and Maintenance Scheduling Agent

Action: 1.The Installation and Maintenance Scheduling Agent performs continuous monitoring of customer services to to prevent recurring faults.

Phase 6: Customer feedback survey

Agent Used: Personal Intelligent Assistant Agent

Action: 1.The Personal Intelligent Assistant Agent schedules the installation/maintenance engineers for service follow-up and review.

4. Security Considerations

TBD

5. IANA Considerations

This document has no IANA actions.

6. 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/info/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/info/rfc8174>.

Acknowledgements

TBD

Authors' Addresses

Yu Fu
China Telecom
Beijing
China
Email: fuy44@chinatelecom.cn

Qing Sun
China Telecom
Beijing
China
Email: sunqiong@chinatelecom.cn

Xin Song
China Telecom
Beijing
China
Email: songx18@chinatelecom.cn

Chongfeng Xie
China Telecom
Beijing
China
Email: xiechf@chinatelecom.cn