Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 20 April 2026

W. Liu, Ed.
Y. Zhang, Ed.
China Unicom

17 October 2025

# Ubiquitous Access Collaboration Requirements for AI Agent Protocols
draft-liu-access-collaboration-agent-00

## Abstract

This document focuses on the ubiquitous access collaboration scenarios, explores the requirements for AI agent communication protocols.

## 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 20 April 2026.

## Copyright Notice

Table of Contents



## 1. Introduction

With the rapid development of AI terminal technology and the popularization of multi scenario networking requirements, scenarios such as home security remote field visits, remote office collaboration, and mixed access of fixed and mobile networks have gradually become the core needs of users. In these scenarios, collaborative interaction between heterogeneous AI agents is the key to realizing service value - for example, in home security scenarios, mobile AI agents need to interact with camera AI agents to transmit real-time images, while linking NAS storage AI agents to save abnormal recordings; In the scenario of mixed access between fixed and mobile networks, the mobile terminal AI agent needs to rely on the fixed network gateway AI agent to achieve seamless network switching and dynamic bandwidth allocation.

However, the effective collaboration of heterogeneous AI agents faces problems such as inconsistent data exchange formats, unstable cross network transmission, and insufficient security verification. These issues directly affect the reliability of service execution: for example, video transmission delays may lead to delayed handling of safety risks for the elderly, and incompatible network configuration information may cause fixed mobile network switching failures. To address these issues, there is an urgent need for a specialized AI communication protocol to provide core support.

This document focuses on the ubiquitous access collaboration scenarios, explores the requirements for AI agent communication protocols.

## 2. Conventions and Definitions

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. Abbreviations and definitions used in this document:

*AI: Artificial Intelligence

## 3. Use Cases

### 3.1. Remote Care

In the scenario of remote access for home security, remote care for the elderly, children, and pets is achieved through the collaboration between mobile terminal AI agents and home fixed network device AI agents (such as cameras, NAS storage, printers, pet sensors). The AI agent communication protocol provides core support for the collaboration between the two. The participating roles include users operating mobile AI agents, mobile AI agents responsible for sending and receiving requests, and home device AI agents executing instructions. When the user checks the status of the elderly, if the phone adjusts the camera screen and there is an abnormality, it triggers the NAS to store the video; When remotely printing materials for children, the phone wakes up the printer; When pets move abnormally, sensors will push alarms, etc. Users can obtain real-time status, normal data transmission, and timely handling of anomalies. The protocol needs to ensure real-time data, request verification, and privacy security.

### 3.2. Remote Work

In remote work scenarios, efficient remote work is achieved through collaboration between terminal AI agents (such as mobile phones and laptops) and office equipment AI agents (such as cloud desktops, printers, video conferencing terminals, file sharing servers). The communication protocol of the AI agents provides core support for the collaboration between the two. The participating roles include employees who operate terminal AI agents, terminal AI agents responsible for command sending and receiving, and office equipment AI agents that execute tasks. When employees need to work, connect the terminal to the cloud desktop; When remotely printing files, the

terminal wakes up the printer; When holding a meeting, the terminal starts the video conferencing terminal and shares files, etc. Employees have access to office resources, stable data transmission, and smooth collaboration. The protocol needs to ensure stable connection, permission control, and data encryption.

### 3.3. Multi Access Collaboration

In the scenario of multi access collaboration, seamless device switching and dynamic allocation of network resources are achieved through the collaboration of mobile terminal AI agents (such as mobile phones and tablets) and fixed network gateway AI agents (such as home optical cats and enterprise routers). The AI agent communication protocol provides core support for the collaboration between the two. The participating roles include users who operate mobile network terminals, mobile network terminal agents responsible for dynamic access, and fixed network gateway agents responsible for resource scheduling. When the user is at home, the mobile network terminal automatically connects to the fixed network gateway to obtain high bandwidth; When going out, the fixed network gateway pushes the network configuration to the mobile network terminal to ensure seamless networking; When multiple devices are accessing simultaneously, the fixed network gateway links with the mobile network terminal to allocate bandwidth resources, etc. Users can achieve seamless network switching, stable device access, efficient resource scheduling, and protocols need to ensure continuous connection, permission control, and bandwidth adaptation.

## 4. Requirement

### 4.1. Identity Authentication and Request Verification

Before executing interaction requests between agents, strict identity authentication must be performed. The protocol shall define high-security authentication mechanisms - such as digital certificates and mutual authentication - to ensure that only legitimate and authorized agents can initiate or receive commands, thereby preventing unauthorized access and malicious control.

### 4.2. Service Discovery and Automatic Negotiation

When an agent accesses a network (e.g., home or office network), it shall automatically discover other available agents and their provided services (e.g., printing, video conferencing, storage). It shall also automatically negotiate capabilities and establish connections to enable "plug-and-play" functionality.

### 4.3. Unified Communication Protocol

A standardized set of message formats, command sets, and interaction workflows shall be defined for inter-agent communication. This ensures that agents from different manufacturers and of different types, e.g., mobile devices, cameras, printers, routers, can identify, understand, and execute commands with one another.

### 4.4. Connection Stability and Seamless Handover

In multi-access collaboration scenarios, when a user switches from a home network to mobile network, the protocol shall support session persistence and seamless handover for agents. This guarantees the uninterrupted operation of ongoing services.

### 4.5. Local Disaster Recovery and Offline Processing Capabilities

In the event of network outages or other anomalies, critical agents (e.g., home gateways, network-attached storage/NAS) shall possess local decision-making and data processing capabilities. For example, after a network disconnection, home sensors shall continue to locally record abnormal events and synchronize the recorded data to the cloud and mobile terminals once the network is restored.

## 5. Security Considerations

TBD

## 6. IANA Considerations

TBD

## 7. 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>.

## Authors' Addresses

Wei Liu (editor)
China Unicom
Beijing
China
Email: liuw550@chinaunicom.cn

Yaomin Zhang (editor)
China Unicom
Beijing
China
Email: zhangym2533@chinaunicom.cn