Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 5 May 2026

J. Mao
G. Zeng
B. Liu
N. Geng
X. Shang
Q. Gao
Z. Li
Huawei Technologies

1 November 2025

Gap Analysis for the Cross-device Communication Protocol for AI Agents in Network Devices
draft-mao-rtgwg-agent-comm-protocol-gap-analysis-00

Abstract

With the development of large language models (LLM), AI Agent software continues to emerge. AI agents deployed on different network devices need to collaborate to accomplish some complex tasks, such as network measurement and network troubleshooting. This collaboration requires cross-device communication between AI agents. The cross-device communication framework is defined in [I-D.mzsg-rtgwg-agent-cross-device-comm-framework].

This document describes whether some classical protocols in networking area, and some popular ones in AI Agent area can be used for the cross-device interaction of the AI agents in network devices, and analyzes the gaps.

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 5 May 2026.

Table of Contents

1. Introduction

With the development of large language models (LLM), AI Agent software continues to emerge. AI agents deployed on different network devices need to collaborate to accomplish some complex tasks, such as network measurement and network troubleshooting. This collaboration requires cross-device communication between AI agents. The cross-device communication framework is defined in [I-D.mzsg-rtgwg-agent-cross-device-comm-framework]

This document describes whether some classical protocols in networking area, and some popular ones in AI Agent area can be used for the cross-device interaction of the AI agents in network devices, and analyzes the gaps.

Currently, network devices are able to exchange message with each other by some routing protocols (e.g. BGP, IS-IS, OSPF), or some signaling protocol (e.g. GRASP). In addition, they can interact with network controller by NETCONF, RESTCONF and gRPC.

In AI Agent area, some popular protocol is worth considering, such as A2A and MCP.

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 RFC 2119 [RFC2119] RFC 8174 [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Terminology

A2A: Agent2Agent Protocol [a2a-link]

MCP: Model Context Protocol [mcp-link]

Device agent: The AI agents deployed in a network device.

GRASP: GeneRic Autonomic Signaling Protocol [RFC8990]

4. Existing Protocols Gap Analysis

Currently, network devices are able to exchange message with each other by some routing protocols (e.g. BGP, IS-IS, OSPF), or some signaling protocol (e.g. GRASP). In addition, they can interact with network controller by NETCONF, RESTCONF and gRPC.

In AI Agent area, there are some popular protocols, such as A2A for interaction between agents and MCP for the interaction between agents and outer systems.

4.1. Gap Analysis for A2A Protocol

* [Gap A01] The content of tasks in A2A protocol is typically described in natural language, and Message and Part objects of the text type in A2A protocol usually carry natural language text. That may require the deployment of large language models on network devices to parse the content of A2A request messages. However, deploying large models requires substantial AI computing capability, which current network devices cannot provide. This suggests that a structured or semi-structured message format or data model may need to be designed.

* [Gap A02] The asynchronous notification mechanism of A2A, which can be used by a server to notify a client that a long-running task has been completed, requires the client to provide a separate listening port or service path as a webhook. This extends the exposure surface of network devices and raises security risks.

* [Gap A03] The first method for A2A service discovery requires an agent to provide a well-known URL to enable other agents to obtain its Agent Card. This increases the exposure surface of network devices and raises security risks. In addition, A2A does not require the retrieval requests for Agent Card to be authenticated, which means that the information of network devices could be accessed by unauthorized users. This suggests that new security mechanisms or service discovery methods may need to be designed to address these security risks.

* [Gap A04] The second method for A2A service discovery requires deploying a registry in the network to store the Agent Cards of all network devices. This means that some network devices need to be selected or newly deployed, and configured to function as registries, similar to the BGP RR. This would lead to significant storage pressure on the device and increase deployment costs. Alternatively, this would require upgrading the network controller to function as a registry, which would cause frequent requests for Agent Cards from devices to the controller, putting additional load on the controller. If the Agent Cards are cached on the devices, there would also be issues of out-of-date cached data and increased storage pressure on the devices.

* [Gap A05] The third method for A2A service discovery requires configuring the Agent Cards of all other devices that will be accessed on the device itself. This would significantly increase the amount of configuration data and the maintenance workload of the network, and also greatly increase the storage pressure on network devices.

* [Gap A06] A2A currently does not mandate a common transport protocol, which allows any of HTTPS-JSON-RPC 2.0, gRPC, or HTTPS-JSON (restful API) to be used. This could actually lead to a situation where the agents in different network devices cannot communicate with each other because of using different transport protocols. This suggests that a standardized transport protocol that must be implemented may need to be specified, with other transport protocols being optional.

* [Gap A07] A2A requires that all messages be transmitted over HTTPS (citation: MUST be HTTPS). This means that each message needs to be encrypted or decrypted in network devices, which imposes additional performance overhead on the devices.

4.2. Gap Analysis for MCP Protocol

* [Gap M01] MCP is typically used by agents to call external systems and is architecturally a north-south interface. However, the relationship among device agents is more like a "peer", similar to BGP peer and IS-IS peer. Their interaction may require an east-west interface. Nevertheless, from the perspective of information transfer and function calling, MCP is also worth considering in the scenario of the interaction of device agents.

* [Gap M02] MCP only supports JSON text as the data encoding format, which is less efficient in terms of information transmission and parsing compared to binary data encoding formats. This will consume more CPU time on devices for data serialization and deserialization, and occupy more bandwidth to exchange messages.

* [Gap M03] MCP allows the use of HTTP protocol stacks that support server-sent events (SSE) and streaming. The protocol stacks of network devices may need to be upgraded accordingly. If devices only support traditional request-response communication, some future functionalities may be limited or impossible to implement.

* [Gap M04] The names and descriptions of MCP tools are in natural language, which may require deploying large language models on network devices to understand the functions of each tool. Currently, the processing capabilities of network devices may be insufficient to meet this requirement. It may be necessary to define a standardized, structured description format or define a standardized tool ID.

4.3. Gap Analysis for GRASP Protocol

TBD

5. Other Protocols Gap Analysis

There are some classical protocols which have been well supported by network devices. If they are going to be used in the scenario of the interaction of device agents, their mechanisms may need to be enhanced, and some data schemas/models may need to be extended or newly defined.

On the other hand, if network devices have basic natural language understanding capability, the data model may be designed as a semi-structured format.

5.1. Gap Analysis for BGP Protocol

TBD

5.2. Gap Analysis for IS-IS Protocol

TBD

5.3. Gap Analysis for OSPF Protocol

TBD

5.4. Gap Analysis for NETCONF Protocol

TBD

5.5. Gap Analysis for RESTCONF Protocol

TBD

5.6. Gap Analysis for gRPC Protocol

TBD

6. IANA Considerations

This document does not include an IANA request.

7. Security Considerations

TBD

8. References

8.1. 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/info/rfc2119>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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>.

8.2. Informative References

[a2a-link] "Agent2Agent Protocol", 30 October 2025, <https://a2a-protocol.org/>.

[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>.

[mcp-link] "Model Context Protocol", 30 October 2025, <https://modelcontextprotocol.io/>.

[RFC8990] Bormann, C., Carpenter, B., Ed., and B. Liu, Ed., "GeneRic Autonomic Signaling Protocol (GRASP)", RFC 8990, DOI 10.17487/RFC8990, May 2021, <https://www.rfc-editor.org/info/rfc8990>.

Authors' Addresses

Jianwei Mao
Huawei Technologies
Beijing
100095
China
Email: MaoJianwei@huawei.com

Guanming Zeng
Huawei Technologies
Email: zengguanming@huawei.com

Bing Liu
Huawei Technologies
Email: leo.liubing@huawei.com

Nan Geng
Huawei Technologies
Email: gengnan@huawei.com

Xiaotong Shang
Huawei Technologies
Email: shangxiaotong@huawei.com

Qiangzhou Gao
Huawei Technologies
Email: gaoqiangzhou@huawei.com

Zhenbin Li
Huawei Technologies
Email: robinli314@163.com