ANIMA
Internet-Draft
Intended status: Standards Track
Expires: 20 July 2026
M. Han, Ed.
N. Zhang, Ed.
J. Zhao, Ed.
China Unicom
16 January 2026

Considerations of AI-powered Autonomic Service Agent Communication

draft-han-anima-ai-asa-01

Abstract

ANIMA defined Autonomic Service Agent to build intelligent management functions into network devices, and could interact with each other through a standard protocol (aka GRASP).With the rapid advancement of Large Language Model (LLM)-driven AI technologies, there is now a potential opportunity to enhance the ASA to be AI-powered, thereby elevating the intelligence of device-built-in management functions to a whole new level.This document analyzes the impact of the AI-powered ASA, mostly from the perspective of the ASA communication protocol.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The ANIMA provides a vision of a network that configures, heals, optimizes, and protects itself. An ASA is defined in [RFC7575] as "An agent implemented on an autonomic node that implements an autonomic function, either in part (in the case of a distributed function) or whole.

[RFC9222] proposes guidelines for the design of Autonomic Service Agents for autonomic networks. Autonomic Service Agents, together with the Autonomic Network Infrastructure, the Autonomic Control Plane, and the GeneRic Autonomic Signaling Protocol, constitute the base elements of an autonomic networking ecosystem.

Large-scale network models have attracted much attention in the field of artificial intelligence in recent years. They integrate the advantages of network technology and LLMs and show great potential in many fields. Especially for network operation and maintenance, it is demonstrating huge enabling potential and providing innovative approaches to solve increasingly complex network operation and maintenance problems.

AI-ASA can achieve more intelligent management functions. Embedding AI-ASA into network devices can enhance operation and maintenance efficiency with LLMs.

This draft analyzes AI-ASA vision and potential functions and describes the scenarios of AI-powered ASA Communication between Network Devices and Network Management Systems. The potential new requirements of GRASP are also discussed.

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.

3. Background

3.1. Definition of ASA

In [RFC8993], ASA is a process that makes use of the features provided by the ANI to achieve its own goals, usually including interaction with other ASAs via GRASP [RFC8990] or otherwise. Of course, it also interacts with the specific targets of its function, using any suitable mechanism. Unless its function is very simple, the ASA will need to handle overlapping asynchronous operations. It may therefore be a quite complex piece of software in its own right, forming part of the application layer above the ANI.

Autonomic Service Agents, together with the Autonomic Network Infrastructure, the Autonomic Control Plane, and the GeneRic Autonomic Signaling Protocol, constitute the base elements of an autonomic networking ecosystem.

3.2. Emergence of AI-powered Agent

[I-D.rosenberg-ai-protocols] Intelligent agent, as an important concept in the field of artificial intelligence, refers to a system that can autonomously perceive the environment, make decisions, and execute actions. It has basic characteristics such as autonomy, interactivity, reactivity, and adaptability, and can independently complete tasks in complex and changing environments. Intelligent agents can learn and make decisions.

[I-D.chuyi-nmrg-ai-agent-network] Al Agent, an automated intelligent entity capable of interacting with its environment, acquiring contextual informationreasoning, self-learning, decision-making, executing tasks (autonomously or in collaboration with other Al Agents) to achieve

There are a few examples of AI Agents.

A travel AI Agent that can help users search for travel destinations based on preferences, compare flight and hotel costs, make bookings, and adjust plans

A loan handling agent that can help users take out a loan. The AI Agent can access a user’s salary information, credit history, and then interact with the user to identify the right loan for the target use case the customer has in mind

A shopping agent for clothing that can listen to user preferences and interests, look at prior purchases, and show users different options, ultimately helping a user find the right sports coat for an event

AI Agent in 3GPP, an automated intelligent entity capable of interacting with its environment, acquiring contextual informationreasoning, self-learning, decision-making, executing tasks autonomously or in collaboration with other AI Agents to achieve a specific goal

4. The Vision of AI-powered ASA

The AI-powered ASA provides more intelligent operation and management of network devices to achieve the Intention-driven network and Auto-driven network.

5. Scenarios of AI-powered ASA Communication between Network Devices

5.1. General

The network devices to communicate with other network devices through anima’s interface.

5.2. Possible Examples

5.2.1. AI Agent based Router for Automatic Congestion Relief

In the automatic congestion relief use case, the traditional solution relies on built-in intelligent modules in devices to implement traffic rerouting via traditional protocols (BGP-LS/BGP-RPD). Device interactions are constrained by predefined protocol rules (e.g., policy triggering based on fixed bandwidth thresholds), lacking cross-device historical data sharing and AI model collaboration. Policy generation depends solely on local TOP-N traffic modeling, unable to adaptively optimize based on real-time traffic patterns.

When AI-powered Agents are introduced into network devices, AI-powered ASA Communication can be established between devices. Devices extend BGP-LS to synchronize real-time link bandwidth and TOP-N traffic characteristics. The AI-powered Agents dynamically define congestion thresholds based on traffic data, replacing manual threshold configuration. Upon detecting congestion, devices use the GRASP protocol to negotiate AI-generated policies (e.g., dynamic adjustment of Multi-Exit Discriminator (MED) values) and route traffic precisely to lightly loaded links via the BGP Routing Process Daemon (BGP RPD). Reinforcement learning is applied to dynamically optimize policy parameters during this process.

5.2.2. AI Agent based Router for Automatic Network DDoS Attacks Defense

With the evolution of attack forms, the Distributed Denial of Service (DDoS) Attacks present the features of short-term and high-frequency outbreaks, and the attack peak value keeps rising year by year, imposing an extreme challenge on the defense response speed. In response to the above attack problems, this document innovatively puts forward an edge defense architecture: deploy attack detection functions to end devices, achieve second-level flash defense against DDoS attacks via intelligent service traffic monitoring, and establish an autonomous network DDoS attack defense system. In the meantime, rely on the AI Agent based Router to support the second-level discovery and real-time interception of attack behaviors, so as to strengthen the network security barrier.

6. Scenarios of AI-powered ASA Communication between Network Management Systems and Devices

6.1. General

The network controller communicates with other netwok devices by the anima interface or protocol.

6.2. Possible Examples

6.2.1. Coordinated IPv6 Monitoring

In the current IPv6 end-to-end traffic monitoring scenario, traffic data collection and analysis rely on manual intervention, while the large volume of live network traffic data results in high resource requirements. When AI-powered Agents are deployed in network controllers and devices, AI-powered ASA communication can be established between IDC controllers and edge devices to enable hierarchical collaboration.

The controller’s AI-powered Agent module discovers network devices via the GRASP protocol, initiates multi-threaded real-time collection and monitoring of IPv6/IP traffic data, and performs preliminary analysis including flow pattern recognition and IPv6/IPv4 traffic ratio trending. Concurrently, the device-side AI-powered Agent collects customer traffic data, decomposes traffic distribution characteristics to identify high-value business scenarios, and synchronizes these insights to the controller via the GRASP protocol. The controller’s AI-powered Agent integrates provincial-level traffic ingress/egress data to construct regional traffic matrices and uploads preliminary analysis results (e.g., internal IDC traffic distribution, inter-provincial link utilization) to the IPv6 end-to-end monitoring platform.

The IPv6 end-to-end monitoring platform leverages multi-dimensional data models to conduct in-depth analysis on the uploaded traffic data and preliminary results, generating final operational decisions such as inter-provincial link bandwidth expansion plans and CDN node deployment recommendations. These decisions are then disseminated to the controller, which issues configuration instructions to the device-side AI-powered Agents via the GRASP API. Upon receiving the instructions, the device’s intelligent module invokes relevant interfaces to adjust server resources and verifies operational effectiveness through self-monitoring threads.

7. Potential New Requirements of GRASP

TBD

7.1. The interface and model extension for Prompt with AI agent

TBD

7.2. Defination of Option for AI-ASA

TBD

8. Security Considerations

Uncertainty of Current AI Technologies.

9. IANA Considerations

TBD

10. References

10.1. 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>.

[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>.

10.2. Informative References

[RFC8993] Behringer, M., Ed., Carpenter, B., Eckert, T., Ciavaglia, L., and J. Nobre, "A Reference Model for Autonomic Networking", RFC 8993, DOI 10.17487/RFC8993, May 2021, <https://www.rfc-editor.org/info/rfc8993>.

[RFC7575] Behringer, M., Pritikin, M., Bjarnason, S., Clemm, A., Carpenter, B., Jiang, S., and L. Ciavaglia, "Autonomic Networking: Definitions and Design Goals", RFC 7575, DOI 10.17487/RFC7575, June 2015, <https://www.rfc-editor.org/info/rfc7575>.

[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>.

[RFC9222] Carpenter, B., Ciavaglia, L., Jiang, S., and P. Peloso, "Guidelines for Autonomic Service Agents", RFC 9222, DOI 10.17487/RFC9222, March 2022, <https://www.rfc-editor.org/info/rfc9222>.

[I-D.rosenberg-ai-protocols] Rosenberg, J. and C. F. Jennings, "Framework, Use Cases and Requirements for AI Agent Protocols", Work in Progress, Internet-Draft, draft-rosenberg-ai-protocols-00, 5 May 2025, <https://datatracker.ietf.org/doc/html/draft-rosenberg-ai-protocols-00>.

[I-D.chuyi-nmrg-ai-agent-network] Guo, C., "Large Model based Agents for Network Operation and Maintenance", Work in Progress, Internet-Draft, draft-chuyi-nmrg-ai-agent-network-02, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-chuyi-nmrg-ai-agent-network-02>.

Authors' Addresses

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

Naihan Zhang (editor)
China Unicom
Beijing
China
Email: zhangnh12@chinaunicom.cn

Jing Zhao (editor)
China Unicom
Beijing
China
Email: zhaoj501@chinaunicom.cn