V6OPS
Internet-Draft
Intended status: Informational
Expires: 15 September 2026

J. Ye
W. Cheng
China Mobile

14 March 2026

Capabilities and Future Requirements of IPv6 for the Internet of Agents (IoA)

draft-yc-ipv6-for-ioa-01

Abstract

In the coming years, the accelerating proliferation of agentic AI is anticipated to drive the number of intelligent agents to reach the scale of hundreds of billions. IPv6, with vast address space, native end-to-end connectivity and rich built-in functionalities, serves as the critical infrastructure underpinning the development of the Internet of Agents (IoA). This draft systematically analyzes the foundational capabilities that IPv6 can provide for the IoA at the current stage, and further explores the evolutionary requirements that the IoA imposes on the future IPv6 development.

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 15 September 2026.

Table of Contents

1. Introduction

As artificial intelligence (AI) technology undergoes a transition from Generative AI to Agentic AI, the global number of AI agents is projected to reach approximately 900 billion by the end of this decade. AI agents, integrating core capabilities such as large language models (LLM), memory systems, tool calling, and task planning, possess the ability to perceive their environment, make autonomous decisions, and execute tasks efficiently, thereby placing new demands on the network infrastructure. Constrained by limited address space, IPv4 struggles to support secure end-to-end connectivity among massive numbers of AI agents. Consequently, the evolution to IPv6-only is not merely a technological upgrade but also a foundational enabler for the large-scale development of agents. As the core protocol for the next-generation Internet, IPv6, with vast address space, native end-to-end connectivity and rich built-in functionalities, serves as the critical infrastructure underpinning the development of the Internet of Agents (IoA).

This draft systematically analyzes the foundational capabilities that IPv6 can provide for the IoA at the current stage, and further explores the evolutionary requirements that the IoA imposes on the future IPv6 development.

1.1. Terminology

1.2. 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.

2. IPv6-Enabled Capabilities for IoA

2.1. Vast Address Space

IPv6 employs a 128-bit address architecture, offering approximately 3.4×10 unique IPv6 addresses, which fundamentally resolves the exhaustion of the IPv4 addresses. In the context of IoA, where a vast number of agents necessitate exact addresses for intercommunication, the expansive address space of IPv6 is of critical importance. It enables the assignment of globally unique addresses to every agent, sensor, or container instance, thereby simplifying service discovery, facilitating horizontal scaling, and allowing for fine-grained identity mapping. As the population of agents grows exponentially, this native capability, which eliminates the need for address reuse, will become the cornerstone supporting a trillion-agent network.

2.2. End-to-End Reachability

The adoption of IPv6 eliminates the dependency on Network Address Translation (NAT), thereby streamlining network design and enabling lower-latency communication. First, the removal of NAT facilitates genuine end-to-end direct communication by assigning a unique global address to each agent. This is essential for the IoA, as it empowers agents to perform point-to-point coordination, task scheduling, and direct orchestration without reliance on intermediate nodes for forwarding or address translation. Furthermore, this end-to-end reachability can reduce the overhead of connection establishment and session lookup introduced by NAT, thereby simplifying coordination protocols among agents and minimizing communication latency.

2.3. SLAAC and Mobility

For certain types of agents, particularly those operating in dynamic environments such as mobile devices, drones and connected vehicles, mobility constitutes a critical characteristic, as these agents frequently need to switch between different network access points. IPv6 provides native support for this requirement through Stateless Address Autoconfiguration (SLAAC).

SLAAC enables devices to autonomously generate IPv6 addresses upon connecting to a network, thereby equipping agents with the capability for rapid network attachment and dynamic readdressing without manual intervention. This realizes "plug-and-play" operation. For systems tasked with managing large-scale deployments of mobile agents, such automated configuration substantially reduces administrative overhead. Moreover, IPv6's robust support in constrained networks further enhances the mobility of edge agents, allowing them to seamlessly roam across access points without communication disruption.

2.4. SRv6 for Remote Management and Path Control

Segment Routing over IPv6 (SRv6) further enhances network intelligence and programmability. By embedding instructions in the IPv6 extension header, SRv6 enables fine-grained path control, allowing the network to dynamically adjust traffic flows based on application requirements. This provides a powerful foundation for the remote management and path optimization of agents. In the context of the IoA, the contributions of SRv6 can be observed across several aspects: First, through flexible path programming, SRv6 enables the establishment of deterministic forwarding paths for packets, thereby achieving ultra-low-latency transmission. This allows agents to rapidly upload locally computed preliminary results to the cloud, realizing the separation of storage and computation while ensuring that raw data remains local and securely isolated. Second, SRv6 supports network slicing, enabling the creation of dedicated virtual networks tailored to diverse agent applications, thereby guaranteeing the quality of service for critical tasks. Third, the integration with application identifiers endows the network with the awareness of upper-layer applications. By embedding application-layer semantic information (e.g., service type, Service Level Agreement (SLA) requirements such as low latency, high bandwidth, and high reliability) directly into IPv6 packets, the network can automatically trigger the corresponding forwarding paths or service function chains.

3. Future Requirements for IPv6

3.1. Elevated Security

The disappearance of NAT, while a advantage of IPv6, also poses new security challenges. In the IPv4 era, NAT unintentionally provided a layer of "obscurity protection" that internal device addresses remained invisible to external network, thereby reducing the risk of direct attacks. With IPv6, however, agents are directly exposed to the public network and are globally addressable, which demands the implementation of more robust host-level security mechanisms. For the IoA, this implies the deployment of finer-grained firewall policies, access control lists (ACLs), and identity authentication. Therefore, it is imperative to establish an advanced security for the IPv6-based IoA to control access based on identity, continuously monitor behaviors, and detect anomalies.

3.2. Privacy and Persistence

The temporary addresses that randomly generated and constantly changed, help protect a topological location and identity from being exposed to eavesdroppers and other information collectors [RFC3041]. However, this pivacy extension also introduces challenges for the communications of agents that require long-lived sessions. In the IoA, persistent connections are often necessary to achieve state synchronization and task continuity, yet the frequent changes of addresses may disrupt the stability of such long-lived sessions.

Striking a balance between privacy protection and session persistence thus emerges as a critical issue for the IoA. On one hand, it is necessary to protect the location, identity, and activities of agents from malicious tracking; on the other hand, it is essential to ensure that the communications of agents performing critical tasks can maintain stability. Addressing this tension may require more sophisticated address management strategies, such as dynamically selecting address types based on task sensitivity and communication patterns, or setting fixed identifiers at the application layer that are independent of addresses.

3.3. Evolution of Threat Defense

The vast address space of IPv6 significantly raises the cost of large-scale attacks that based on address scanning. Attackers can no longer enumerate all possible addresses as easily as in IPv4 space, even the state-of-the-art academic scanning tools can only discover tens of millions of IPv6 hosts within the 2^128 address space. However, they may also exploit IPv6-specific features (e.g., IPv6 extension header, Neighbor Discovery Protocol (NDP)) to launch novel attacks, or leverage the vast address space to rapidly mutate source addresses and evade detection. Therefore, threat defense strategies

must be reassessed in the IPv6 era.

In the IoA, IPv6 provides abundant address resources for agents, yet the increasing proliferation of agents and IoT devices may become new attack sources and could be potentially exploited to amplify attack. Traffic analysis and scrubbing as the core traditional DDoS defense, face significant challenges in meeting real-time analysis and scrubbing requirements due to the far greater complexity of IPv6 protocol types and address structures compared to IPv4. Legacy scrubbing mechanisms, originally designed for simple packet characteristics in IPv4 environments, are now required to perform deep parsing and exact matching of complex IPv6 addresses within massive traffic flows, leading to a surge in processing overhead for existing security devices.

SRv6 carries programmable path, enabling on-demand service assurance and customized quality of service for agent-based applications. However, this mechanism can be abused to launch various targeted attacks. For instance, an attacker may craft SRv6 packets with excessively long Segment Lists, forcing intermediate endpoints to consume substantial CPU resources to farse extension header; By tampering with the SRH, an attacker can cause packets to bypass specific nodes (e.g., accounting nodes, security service nodes); Or attackers maliciously construct looping paths (e.g., A→B→C→A) to exhaust bandwidth, resulting in exponential traffic amplification in multi-agent collaboration. Therefore, to better support the implementation of IoA, the design and deployment of SRv6 security mechanisms must be accelerated.

To effectively support the Internet of AI Agents, security capabilities must be strengthened through a three perspectives: first, refining threat detection rules for IPv6-specific attacks, including NDP spoofing, extension header manipulation, and fragment attacks; second, expediting the enhancement of SRv6 security mechanisms; and third, upgrading security devices with AI-powered real-time traffic analysis to enable rapid anomaly detection, thereby bolstering the real-time performance and accuracy of defenses against increasingly intelligent attacks in the IPv6 environment.

3.4. Monitoring and Management

Building an IPv6-based comprehensive network observability framework is essential to better support the efficient operation of the Internet of Agents (IoA). This requires the establishment of IPv6-native telemetry and monitoring capabilities, along with corresponding updates to threat detection rules. However, current monitoring systems provide insufficient support for IPv6, with many legacy tools exhibiting deficiencies in handling IPv6 formats,

extension headers, and specific behaviors. For instance, the IPv6 Flow Label field, which can be used to mark traffic priority at the packet level, remains largely underutilized by existing monitoring tools. Meanwhile, the address changes introduced by privacy extensions render traditional address-based tracking and auditing methods ineffective, further undermining network visibility. Furthermore, inconsistencies in the processing of IPv6 extension headers introduce additional complexity to network monitoring: Different devices handle IPv6 packets with extension headers in varied ways. For example, some may forward them normally, others may silently ignore them, and some may even discard them outright.

Therefore, data sampling and monitoring tools must be fully adapted to IPv6, ranging from correct interpretation of extension header semantics to the effective utilization of various specialized fields, so as to ensure continuous observation and analysis of agents' operations and behaviors, as well as timely anomaly detection.

4. Security Considerations

TBD.

5. IANA Considerations

This document has no IANA actions.

6. References

6.1. 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>.

6.2. Informative References

[RFC3041] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, DOI 10.17487/RFC3041, January 2001, <https://www.rfc-editor.org/rfc/rfc3041>.

Acknowledgements

Contributors

Authors' Addresses

Jiaming Ye
China Mobile
Email: yejiaming@chinamobile.com

Weiqiang Cheng
China Mobile
Email: chengweiqiang@chinamobile.com