

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

draft-yc-ipv6-for-ioa

Jiaming Ye(China Mobile)(Presenter)

Weiqiang Cheng(China Mobile)

IETF-125, Mar 2026

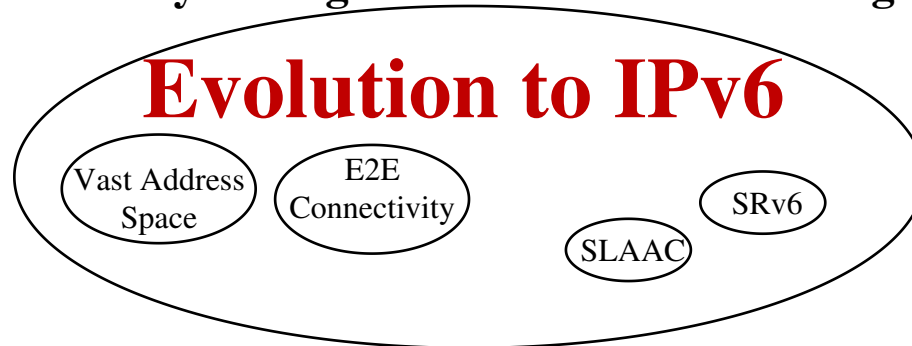
Background

- **AI Agent:** an intelligent entity that senses its environment, reason about goals and acts autonomously to complete tasks.
- **Internet of Agents (IoA):** autonomously discover, interact and collaborate with humans, other agents, and tools, driving intelligent and autonomous evolution of the Internet.
- **Explosion of Agents:** projected to reach hundreds of billions in the near term

Background

- **AI Agent:** an intelligent entity that senses its environment, reason about goals and acts autonomously to complete tasks.
- **Internet of Agents (IoA):** autonomously discover, interact and collaborate with humans, other agents, and tools, driving intelligent and autonomous evolution of the Internet.
- **Explosion of Agents:** projected to reach hundreds of billions in the near term

Constrained by **limited address space, IPv4 struggles to support** secure end-to-end connectivity among massive numbers of AI agents

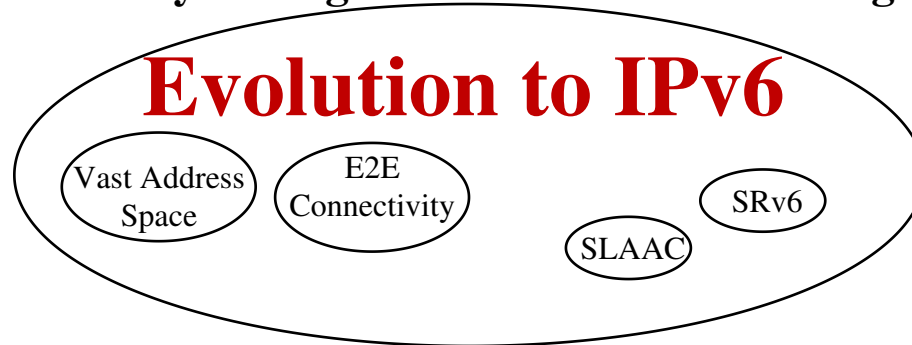


Background

- **Explosion of Agents:** projected to reach hundreds of billions in the near term



Constrained by **limited address space, IPv4 struggles to support** secure end-to-end connectivity among massive numbers of AI agents



- This draft 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

IPv6-Enabled Capabilities for IoA

Evolution to IPv6 is not merely a technological upgrade but also a foundational enabler for the large-scale development of agents:

✓ Vast Address Space (3.4×10^{38})

- A vast number of agents necessitate exact addresses for intercommunication
- Enable the assignment of globally unique addresses to every agent, or sensor, eliminating the need for address reuse

✓ End-to-End Reachability

- Eliminates the dependency on NAT



- Empower agents' point-to-point coordination and direct orchestration without reliance on intermediate nodes for forwarding or address translation
- Reduce the overhead of connection establishment and session lookup introduced by NAT, thereby minimizing communication latency

IPv6-Enabled Capabilities for IoA

✓ SLAAC and Mobility

- Agents operating in dynamic environments (e.g. mobile devices, drones, connected vehicles), critically depend on mobility for frequently switching between different network access points
- 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

✓ SRv6 for Remote Management and Path Control

- Enhance network intelligence and programmability, providing a foundation for the remote management and path optimization of agents.
 - ↓
 - Enable deterministic forwarding paths for packets, ensuring packets traverse the network with specific performance metrics. (e.g. ultra-low latency, high bandwidth, high throughput, zero packet loss...)
 - Aware of upper-layer applications by embedding application-layer semantic information in application identifiers (e.g., service type, performance requirements), automatically triggering the corresponding forwarding paths or SFC

Future Requirements for IPv6

Elevated Security

- Disappearance of NAT makes agents directly exposed to the public network and are globally addressable
- Establish an advanced security (finer-grained firewall policies, ACLs, identity authentication) for the IPv6-based IoA to control access based on identity, monitor behaviors, and detect anomalies

Privacy and Persistence

- Privacy extension (temporary addresses) help protect a topological location and identity from being exposed to information collectors
- Some agents require long-lived sessions to achieve state synchronization and task continuity
- More sophisticated address manage: dynamically selecting address types based on task sensitivity and communication patterns, or setting fixed identifiers at the application layer that are independent of addresses

Future Requirements for IPv6

Evolution of Threat Defense

- New attacks are emerging that exploit IPv6-specific features:
 - Insufficient traffic analysis and scrubbing performance due to IPv6 address complexity (long addresses, vast address space, rich semantics)
 - Evolving SRv6 security mechanisms vulnerable to malicious header tampering (e.g. overly long segment lists, path loops causing bandwidth exhaustion and traffic amplification)
- Enhance threat defense from 3 perspectives:
 - Refine threat detection rules and improve traffic scrubbing performance for IPv6-specific attacks
 - Accelerate the design and deployment of SRv6 security mechanisms
 - Introduce AI-driven real-time traffic analysis systems (adaptively learn behavior and rapidly identify anomalies, boost defense accuracy and responsiveness)

Future Requirements for IPv6

Monitoring and Management

- Current monitoring systems provide insufficient support for IPv6. (Inconsistent handling of packets, insufficient utilization of specific fields, temporary addresses hindering traceability)
- Building an comprehensive IPv6-native network observability to ensure continuous agent visibility and timely anomaly detection

Questions?

- Any questions or comments are welcome.

Thanks!