v6ops
Internet-Draft
Intended status: Best Current Practice
Expires: 3 September 2026

R. Pang
J. Zhao
China Unicom
M. Jin
Huawei
S. Zhang
China Unicom

2 March 2026

IPv6 Network Deployment Monitoring and Analysis
draft-pang-v6ops-ipv6-monitoring-deployment-05

Abstract

This document addresses key operational challenges in large-scale IPv6 deployment and proposes an architecture for IPv6 deployment monitoring and analysis. It describes an architectural approach and comprehensive metrics to provide end-to-end visibility across network infrastructure, cloud services, edge computing, and end-user domains.

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 3 September 2026.

Copyright Notice

Table of Contents

1. Introduction

The IPv6 protocol specification was published in 1998. As IPv6 adoption has accelerated in recent years, IPv6 was standardized as an Internet Standard [RFC8200] in 2017.

1.1. Current IPv6 Deployment Status

The deployment of IPv6 has become a core driving force for network development. With the continuous expansion of network scale and the emergence of new services, IPv6 provides abundant address space, enhanced security, and improved network performance, making it a key component in network evolution. The efficient deployment and promotion of IPv6 networks have become critical priorities for operators and service providers.

As of 2023, significant progress has been made in global IPv6 deployment. According to the _Global IPv6 Development Report 2024_ [GlobalIPv6Report2024], IPv6 deployment accelerated notably in 2023, with global coverage exceeding 30% for the first time. In leading countries, IPv6 coverage has reached or approached 70%, and the proportion of IPv6 mobile traffic has surpassed that of IPv4.

[RFC9386] describes the IPv6 deployment status in 2022, and Section 5 lists common challenges including transition mechanisms, network management and operation, performance, and customer experience. ETSI-GR-IPE-001 [ETSI-GR-IPE-001] also analyzes existing gaps in IPv6-related use cases.

1.2. Current Approaches to Monitoring IPv6 Deployment

Several tools and platforms are used to monitor IPv6 deployment, such as:

* Internet Society Pulse: Curates information about IPv6 adoption levels in countries and networks worldwide.

* Akamai IPv6 Adoption Visualization: Tracks IPv6 adoption trends at country or network level.

* APNIC IPv6 Measurement: Provides an interactive map for viewing IPv6 deployment rates in specific countries.

* Cloudflare IPv6 Adoption Trends: Offers IPv6 adoption insights across the Internet.

* Cisco 6lab IPv6: Displays IPv6 prefix data.

* Regional or National Monitoring Platforms: Examples include NZ IPv6, RIPE NCC IPv6 Statistics, and USG IPv6 & DNSSEC External Service Deployment Status.

While valuable for high-level trend analysis, these tools have significant limitations for carrier-grade operational use.

Inadequate IPv6 monitoring can lead to unrecognized service degradation, increased operational costs, and poor end-user experience, which hinders the large-scale adoption of IPv6.

2. Problem Statement

2.1. Fragmented Monitoring Coverage

Monitoring points are predominantly concentrated in backbone networks [RFC7707], lacking fine-grained visibility into user terminals, access networks, and application endpoints.

2.2. Single-Dimensional Evaluation

Assessments mainly rely on basic metrics such as connection availability [RFC9099] and address allocation rates, lacking a holistic view of service continuity, transmission quality, network element readiness, and active connection states.

2.3. Lack of Cross-Domain Correlation

Data silos exist among different network domains (fixed, mobile, core, application), preventing end-to-end path analysis and fault correlation [RFC9312].

2.4. Insufficient In-Depth Analysis

Incomplete IPv6 transformation in applications and content delivery chains (e.g., deeply nested links, multimedia content) is difficult to characterize without in-depth monitoring capabilities for such scenarios.

2.5. Limited Dynamic Prediction

Current models cannot effectively quantify the impact of external factors (policy changes, user behavior, market dynamics) on IPv6 evolution, which limits proactive network planning.

3. IPv6 Network End-to-End Monitoring and Analysis Architecture

To address the above challenges, this document describes an end-to-end IPv6 monitoring and analysis architecture. The architecture provides full visibility into IPv6 deployment while ensuring interoperability and scalability.

3.1. Architectural Principles

The monitoring framework follows these key principles:

* Standardized Data Models: Use standardized data models (e.g., YANG) for consistent data representation across domains to ensure interoperability.

* Modular Design: Deploy independent functional components with well-defined interfaces to support incremental deployment.

* Cross-Domain Correlation: Enable end-to-end visibility via integrated data analysis across administrative domains.

* Service-Oriented Metrics: Use a comprehensive monitoring metrics framework aligned with operational objectives.

* Visualization Tools: Dashboards and visual interfaces to support key operational decisions.

* Extensibility: Support integration with existing monitoring systems and allow future extensions.

3.2. Architecture Components

The architecture consists of three layers, as shown in Figure 1: the Data Collection Layer, the Intelligent Analysis Layer, and the Visualization Layer.

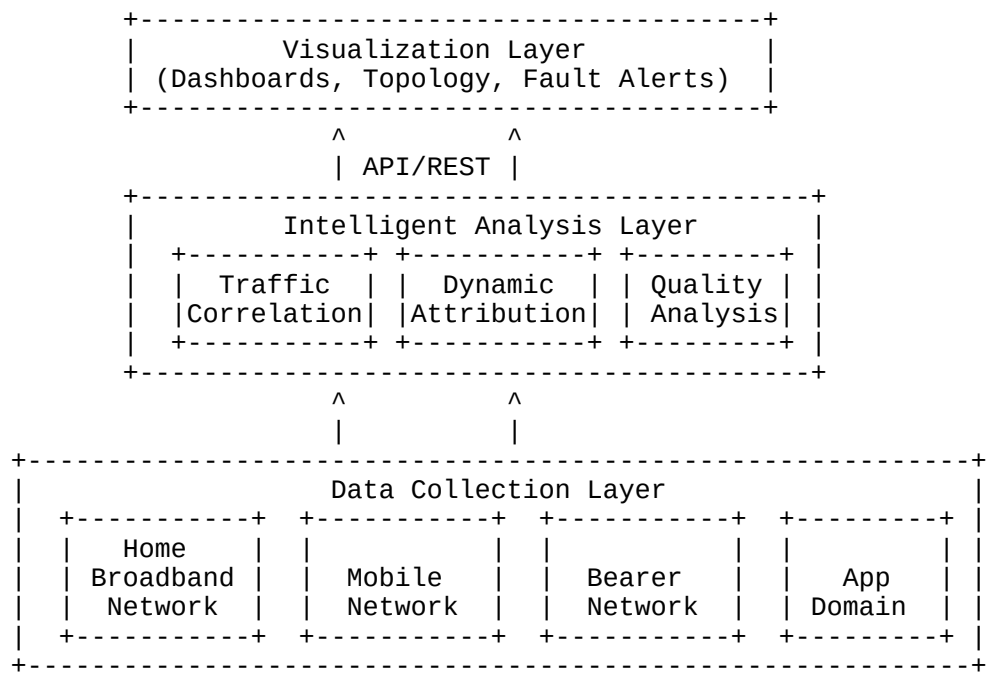

Figure 1: IPv6 Network End-to-End Monitoring and Analysis Architecture

3.2.1. Data Collection Layer

This layer defines unified interface standards to integrate multi-source data from the home broadband network, mobile network, IP bearer network, and application domain. The framework supports interworking with multi-vendor devices and subsystems.

Implementations SHOULD leverage existing IETF standards for data collection where applicable.

* Integration with existing network management systems can provide daily-level monitoring data through standardized interfaces.

* The architecture leverages mature, standardized collection mechanisms (such as Telemetry, NETCONF/YANG etc.) to ensure uniform data formats and meet high-frequency traffic monitoring requirements.

3.2.2. Intelligent Analysis Layer

The Intelligent Analysis Layer processes traffic data collected from the four major service domains. Using multi-dimensional traffic analysis models and comprehensive metrics, it provides fine-grained insights and supports cross-domain root cause diagnosis. This layer also supports AI-based model extensions, including anomaly detection for unexpected drops in IPv6 traffic and predictive analytics for forecasting IPv6 traffic growth based on historical data and external factors (e.g., regional policy rollouts).

3.2.2.1. Multi-domain Traffic Correlation Analysis

* Network Traffic Analysis: Supports collection of IPv6/IPv4 inbound and outbound traffic at key network nodes. Analyzes traffic evolution trends.

* User-Side Traffic Analysis: Monitors user-side devices and access networks (fixed and mobile), including IPv6 capability monitoring of home ONTs, routers, end-user devices, and access networks.

* Application Traffic Analysis: Supports collection and analysis of IPv6/IPv4 active applications, and calculates IPv6 traffic for different services.

* Inter-network Traffic Analysis: Builds region-application matrices to analyze cross-operator paths and locate regional bottlenecks.

3.2.2.2. Dynamic Traffic Attribution

Based on traffic analysis results from each domain, this component identifies regions with anomalous IPv6 traffic. Using multi-domain correlation analysis (e.g., by region, network layer, or application type), it attributes traffic fluctuations to specific subsystems.

Optionally, monitoring insights can inform network policy adjustments that influence client-side path selection behaviors, such as those defined in Happy Eyeballs [RFC8305].

3.2.2.3. Traffic Quality Analysis

* User-level Topology Reconstruction: Models service chains and reconstructs end-to-end topologies, supporting segmented diagnosis of latency and packet loss (home terminal, access network, application segments).

* Deterioration Localization: Compares IPv4/IPv6 performance segment by segment to locate underperforming network elements.

* IPv6 Application Access Quality Assessment: Evaluates KPIs of application systems in IPv6 environments, including response time, connection success rate, and data transmission rate.

3.2.3. Visualization Layer

The Visualization Layer presents analyzed data via operational dashboards to support network management decisions.

Key functions include:

* Unified Operational Dashboard: Presents an overview of key IPv6 deployment metrics and ecosystem trends using real-time widgets, charts, and graphs.

* Cross-Domain Topology Views: Displays interactive topology maps for each network domain, showing the status of IPv6-enabled resources, connections, and operational state.

* Multi-Dimensional Data Exploration: Provides chart-based views (traffic distribution, quality trends, application support comparison etc.) that allow operators to filter metrics by time, region, service type, and other dimensions.

* Fault and Status Visualization: Converts root cause analysis results into visual alerts on dashboards and topologies (color-coded nodes, heat maps etc.) to speed up fault identification and troubleshooting.

3.2.4. IPv6 Monitoring Metrics

The comprehensive IPv6 monitoring metrics framework includes the following categories:

* Readiness Metrics

  - Network Element Readiness: IPv6 readiness of network equipment, end-user devices, and security devices.

  - Application Readiness: IPv6 support rates for websites and service systems.

  - Infrastructure Readiness: IPv6 readiness of fixed Internet, mobile Internet, dedicated lines, and data center network (DCN) infrastructure.

  - Network Readiness:

    - o IPv6 coverage of backbone networks, metropolitan area networks (MANs), IDCs, and dedicated lines.

    - o End-to-end IPv6 performance of backbone networks, MANs, IDCs, dedicated lines, and access networks.

  - Cloud Readiness: IPv6 readiness of CDNs, cloud services, cloud platforms, and DNS servers.

* Operational Metrics

  - IPv6 Traffic: IPv6 traffic share in cross-border, inter-domain, intra-domain, fixed MAN, mobile core, IDC, dedicated line, and application traffic.

  - Active IPv6 Connections: IPv6 active connection share in fixed MAN, mobile core, IDC, dedicated line, and application services.

* Performance and Quality Metrics

  - DNS Resolution Latency and Success Rate.

  - End-to-End Latency (RTT).

  - Packet Loss Ratio (PLR).

4. Implementation Considerations

This architecture and its associated metrics have been deployed in operational networks, delivering measurable improvements in IPv6 deployment effectiveness. Based on experiences from large-scale operator networks, the following key recommendations are provided:

4.1. Phased Deployment Strategy

1. Phase 1: Prioritize monitoring of key nodes in core and metro networks to quickly obtain basic IPv6 traffic visibility.

2. Phase 2: Extend to user-side terminal collection and application-side active probing to establish end-to-end monitoring capabilities.

3. Phase 3: Enhance intelligent analysis models to support automated root cause localization and predictive analytics.

4.2. Organizational Collaboration Model

* Establish cross-departmental teams (fixed, mobile, IP bearer, application etc.) to ensure data sharing and process integration.

* Define data ownership for each domain and establish data quality governance mechanisms.

4.3. Technical Selection Recommendations

* Prioritize network devices that support standard interfaces (NETCONF/YANG, Telemetry) to reduce integration complexity.

* Adopt a modular architecture to facilitate future function expansion and multi-vendor access.

4.4. Deployment Validation

The architecture and metrics described in this document have been deployed on the operational networks of major operators (e.g., China Unicom), covering fixed broadband, mobile, IP bearer, and application domains.

5. Security Considerations

Implementations MUST provide:

* Role-based access control.

* Anonymization of user-related data.

* Secure data transmission protocols.

* Integrity verification for collected metrics.

The monitoring mechanism described in this document uses passive monitoring only. It does NOT modify, insert, or delete any IPv6 or IPv4 packet headers, payloads, or user traffic. No changes are made to packet content or format during collection and analysis, ensuring user traffic integrity and no impact on network services. No personally identifiable information (PII) is collected, processed, or reported, thus eliminating end-user privacy risks.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

7.2. Informative References

[RFC7707] Gont, F. and T. Chown, "Network Reconnaissance in IPv6 Networks", RFC 7707, DOI 10.17487/RFC7707, March 2016, <https://www.rfc-editor.org/info/rfc7707>.

[RFC8305] Schinazi, D. and T. Pauly, "Happy Eyeballs Version 2: Better Connectivity Using Concurrency", RFC 8305, DOI 10.17487/RFC8305, December 2017, <https://www.rfc-editor.org/info/rfc8305>.

[RFC9099] Vyncke, ., Chittimaneni, K., Kaeo, M., and E. Rey, "Operational Security Considerations for IPv6 Networks", RFC 9099, DOI 10.17487/RFC9099, August 2021, <https://www.rfc-editor.org/info/rfc9099>.

[RFC9312] Khlewind, M. and B. Trammell, "Manageability of the QUIC Transport Protocol", RFC 9312, DOI 10.17487/RFC9312, September 2022, <https://www.rfc-editor.org/info/rfc9312>.

[RFC9386] Fioccola, G., Volpato, P., Palet Martinez, J., Mishra, G., and C. Xie, "IPv6 Deployment Status", RFC 9386, DOI 10.17487/RFC9386, April 2023, <https://www.rfc-editor.org/info/rfc9386>.

[GlobalIPv6Report2024] "Global IPv6 Development Report 2024", n.d..

[ETSI-GR-IPE-001] "IPv6 Implementation Gaps and Recommendations", n.d..

Authors' Addresses

Ran Pang
China Unicom
Beijing
China
Email: pangran@chinaunicom.cn

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

Mingshuang Jin
Huawei
Beijing
China
Email: jinmingshuang@huawei.com

Shuai Zhang
China Unicom
Beijing
China
Email: zhangs366@chinaunicom.cn