v6ops
Internet-Draft
Intended status: Standards Track
Expires: 23 April 2026

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

20 October 2025

IPv6 Network Deployment Monitoring and Analysis
draft-pang-v6ops-ipv6-monitoring-deployment-03

Abstract

This document identifies key operational challenges in large-scale IPv6 deployment and proposes a set of proven, integrated monitoring and analysis frameworks to address them. By establishing a standardized architecture and a comprehensive evaluation index system, it enables end-to-end visibility across cloud, network, edge, and end systems. This document provides complete operational guidance from data collection and cross-domain correlation to intelligent analysis and bottleneck identification, offering executable solutions for operators to accelerate IPv6 deployment. The described best practices have been validated in the live networks of major operators, achieving significant improvements in IPv6 traffic.

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 23 April 2026.

Table of Contents

1. Introduction

The emergence of IPv6 can be traced back to the 1990s, when the development of IPv6 was initiated by the Internet Engineering Task Force (IETF) to solve the problem of IPv4 address exhaustion. In 1998, the IPv6 protocol specification was published. AAs IPv6 adoption has been accelerating over the past years, the IPv6 protocol was elevated to be an Internet Standard status [RFC8200] in 2017.

1.1. Current IPv6 Deployment Status

In today's digital age, 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 applications, the extensive address space, enhanced security, and improved network performance of IPv6 have made it a key element in network evolution. How to better deploy and promote IPv6 networks has become a widely concerned issue.

As of 2023, significant strides have been made in the global deployment of IPv6. According to the statistics from the 'Global IPv6 Development Report 2024', in 2023 the deployment of IPv6 networks significantly accelerated, breaking through the 30% mark in global coverage for the first time. Among leading countries, the IPv6 coverage rate has reached or approached 70%, and the percentage of IPv6 mobile traffic has surpassed that of IPv4.

[RFC9386] presents the state of IPv6 network deployment in 2022, and its Section 5 lists common challenges, such as transition mechanisms, network management and operation, performance, and customer experience. 'ETSI-GR-IPE-001' also discusses the existing gaps in IPv6-related use cases.

1.2. Current Approaches to Monitoring IPv6 Deployment

Several tools and platforms monitor IPv6 deployment, such as:

* Internet Society Pulse: Curating information about levels of IPv6 adoption in countries and networks around the world.

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

* APNIC IPv6 Measurement: Providing an interactive map that users can click on to see the IPv6 deployment rate in a particular country.

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

* Cisco 6lab IPv6: Displaying IPv6 prefix data.

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

While valuable for high-level trend analysis, these tools exhibit significant limitations for operational purposes.

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 primarily rely on basic metrics like 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 between different network domains (e.g., fixed, mobile, core, application), preventing end-to-end path analysis and fault correlation [RFC9312].

2.4. Insufficient In-Depth Analysis

Incomplete IPv6 transformation in private applications and content delivery chains (e.g., secondary/tertiary links, multimedia content) remains difficult to detect, as deep monitoring capabilities for these scenarios are lacking.

2.5. Limited Dynamic Prediction

Current models struggle to quantify the impact of external factors (e.g., policy changes, user behavior, market dynamics) on IPv6 evolution, limiting proactive planning.

3. Framework for IPv6 Deployment Monitoring Analysis

This framework is designed to overcome the above challenges through the following core principles:

* Unified Data Collection: Standardized interfaces for cross-domain data ingestion.

* Correlation analysis: Integrated data fusion and cross-domain analytics.

* Service-Oriented Metrics: A comprehensive indicator system aligned with business objectives.

* Visualized operation: Dashboards and visual tools to support key operational decisions.

* Extensibility: Leverages existing monitoring infrastructure and supports integration with external systems.

3.1. IPv6 Network End-to-End Monitoring and Analysis System Architecture

The system architecture is divided into three layers from top to bottom (shown in Figure 1): the Data Collection Layer, the Intelligent Analysis Layer, and the Visualization Layer.

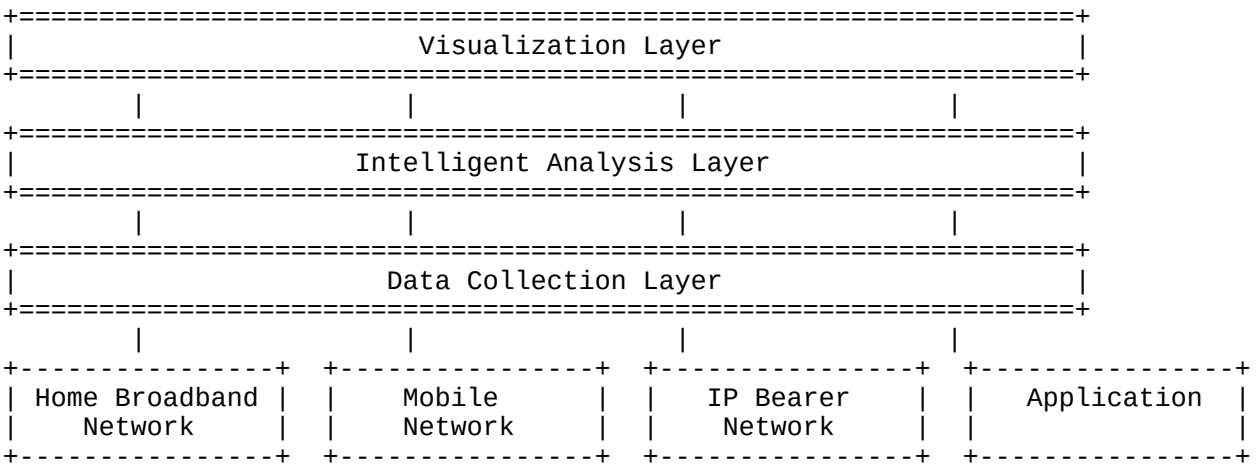

Figure 1: IPv6 Network End to End Monitoring and Analysis System

3.1.1. Data Collection Layer

Defines unified interface standards to integrate multi-source data from user, network, and application sides, ensuring compatibility with multi-vendor devices and subsystems.

Data collection relies on the existing technical system. The specific methods are:

* Adopt the established standardized data collection mechanism to ensure the uniformity of data formats.

* Access the existing network management systems of each professional network, and realize automatic collection and synchronization of indicator data through interface docking.

3.1.2. Intelligent Analysis Layer

Develops multi-dimensional traffic analysis models to enable granular insights and cross-domain root cause diagnosis.

3.1.2.1. Multi-domain Traffic Correlation Analysis

* Multi-domain Traffic Correlation

  - Network traffic analysis: Supports collection of IPv6/IPv4 inbound and outbound traffic at key network nodes. Analyze traffic change trends.

  - Application traffic analysis: Supports collection and analysis of IPv6/IPv4 active applications on the user side and application side. Calculates IPv6 traffic data for different service applications.

  - Inter-network traffic analysis: Constructs region-application matrices to analyze cross-operator paths and identify regional bottlenecks.

* Dynamic traffic attribution

  - Identifies traffic-constrained areas, formulates multi-dimensional investigation plans (network, user, application), and attributes traffic fluctuations to specific subsystems.

3.1.2.2. Quality Deterioration Delimitation and Topology Restoration

* User-level Topology Reconstruction: Models service chains to reconstruct end-to-end topologies, enabling segmented diagnosis of latency/packet loss (e.g., home terminal, access network, application segments).

* Segmented Quality Degradation Localization: Compares IPv4/IPv6 performance segment-by-segment to pinpoint degraded network elements.

3.1.3. Visualization Layer

Provides indicator-based presentation and decision support.

3.1.3.1. Indicator-Based Presentation

Monitors and analyzes IPv6 support across domains, decomposing metrics by business and network segment.

3.1.3.2. Decision Support

3.2. Indicator System

Based on a standardized indicator system, conduct IPv6 support monitoring and analysis for each professional domain, breaking down monitoring metrics into specific services and network segments.

* Readiness Indicators

  - Network Element Readiness: IPv6 Readiness of Network Equipment, End-User Devices, and Security Devices.

  - Application Readiness: IPv6 Support Rate of Website Applications and Business Systems.

  - Infrastructure Readiness: IPv6 Readiness of Fixed Internet, Mobile Internet, Private Lines, and Data Center Network (DCN) Infrastructure.

  - Network Readiness:

    o IPv6 Network Coverage of Backbone Networks, Metropolitan Area Networks (MANs), Internet Data Centers (IDCs), and Private Lines.

    - o End-to-End IPv6 Network Performance of Backbone Networks, Metropolitan Area Networks (MANs), Internet Data Centers (IDCs), Private Lines, and Access Networks.

  - Cloud Readiness: IPv6 Readiness of Content Delivery Networks (CDNs), Cloud Services, Cloud Platforms, and DNS Servers.

* Operational Metrics

  - IPv6 Traffic: IPv6 Traffic Share in Cross-Border, Inter-Domain, Intra-Domain, Fixed Metropolitan Area Networks (MANs), Mobile Core Networks, Internet Data Centers (IDCs), Private Lines, and Applications.

  - Active IPv6 Connections: Active IPv6 Connection Share in Fixed Metropolitan Area Networks (MANs), Mobile Core Networks, Internet Data Centers (IDCs), Private Lines, and Applications.

* Quality Metrics

  - DNS Resolution Performance

  - End-to-End Latency

  - Packet Loss Ratio

* Policy Compliance Indicators

4. Scenario-Based Capability Examples

4.1. IPv6 Monitoring and Analysis on the User Side

Monitor and analyze data from fixed and mobile network user sides, including: IPv6 support monitoring and IPv6 traffic quality analysis. Support end-to-end data analysis at the intelligent analysis layer.

4.2. IPv6 Support and Application Access Quality Monitoring for Application Systems

Through application monitoring points, monitor and analyze the IPv6 support of application systems, including: website and APP monitoring, IPv6 application access quality evaluation, and DNS resolution capability monitoring.

TBD.

5. Use cases

5.1. User Network Quality Issue Localization

* Scenario: User A experiences lag during cloud gaming at home.

* Challenge: Isolating the cause requires correlating performance data across multiple segments (N1: terminal to ONT; N2: ONT to BRAS; N3: BRAS to application), but domains are independently managed.

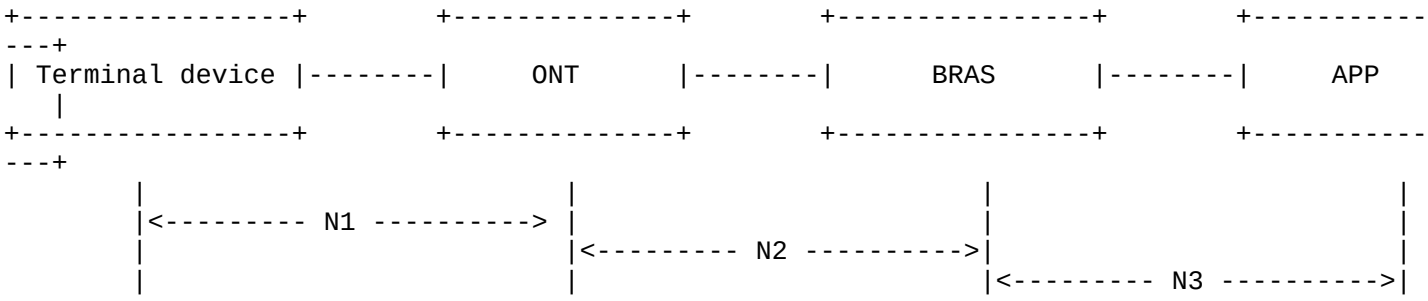

Figure 2: Network schematic diagram based on home broadband network access application

* Solution: The system detected end-to-end quality degradation. Using segmented analysis, it pinpointed abnormal latency in the N3 segment. Correlation with CDN logs revealed a content source switch from a local IDC to a remote cross-province node.

* Conclusion: Quality degradation was caused by CDN remote scheduling and N3 inter-network link congestion.

* Action: Adjusting CDN scheduling strategy resolved the issue.

* Effectiveness: This approach reduced the average fault localization time for similar issues from hours to minutes.

5.2. Home terminals and routers Traffic Analysis

* Solution: The System detected below-average IPv6 traffic share in a demo community.

* Investigation: Correlation with terminal data showed a high proportion of bridge-mode optical network terminals (ONTs) and older routers supporting only IPv4/NAT.

* Root Cause: Legacy routers forced IPv6 traffic to fall back to IPv4.

* Action: Targeted replacement of bridge-mode ONTs with router-mode ONTs and upgrading old routers.

* Effectiveness: After implementation, the community's IPv6 traffic share increased from 15% to 45% within two weeks.

6. Implementation Considerations

Based on deployment experience in major operator networks, we summarize the following key implementation recommendations:

6.1. Phased Deployment Strategy

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

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

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

6.2. Organizational Collaboration Model

* Establish cross-departmental (fixed, mobile, data center) joint teams to ensure data sharing and process integration.

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

6.3. Technical Selection Recommendations

* Prioritize network devices supporting standard interfaces (e.g., NETCONF/YANG, Telemetry) to reduce integration complexity.

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

7. Security Considerations

The monitoring system must implement:

* Role-based access control.

* Anonymization of user-specific data.

* Secure data transmission protocols.

* Integrity verification for collected metrics.

8. IANA Considerations

TBD.

9. References

9.1. 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>.

9.2. 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>.

[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>.

Authors' Addresses

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

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

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

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