v6ops
Internet-Draft
Intended status: Standards Track
Expires: 5 January 2026

R. Pang, Ed.
J. Zhao, Ed.
China Unicom
M. Jin, Ed.
Huawei
S. Zhang, Ed.
China Unicom
4 July 2025

IPv6 Network Deployment Monitoring and Analysis
draft-pang-v6ops-ipv6-monitoring-deployment-01

Abstract

This document presents an IPv6 network end-to-end monitoring and analysis system. It describes a standardized end-to-end monitoring and analysis architecture and an indicator system, while also enabling capabilities for end-to-end monitoring data collection and integrated intelligent analysis. This solution has been verified in the operators' network.

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 5 January 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. As IPv6 adoption 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

Existing IPv6 deployment monitoring approaches include (not an exhaustive list):

* 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.

The aforementioned tools are capable of providing effective statistics and visualization of IPv6 support levels. However, they do not adequately address the key problems that currently exist. The specific deficiencies are presented in the following five aspects.

2. Problem Statement

2.1. Fragmented Monitoring Coverage

Existing monitoring points are concentrated in the backbone network [RFC7707], lacking fine-grained coverage of terminals and applications.

2.2. Single-Dimensional Evaluation

It mainly relies on basic indicators such as connection availability [RFC9099] and address allocation rate, lacking a comprehensive assessment of service continuity, transmission quality, Network Element Readiness, Active IPv6 Connections, and other key metrics.

2.3. Lack of Cross-Domain Correlation

The monitoring data of each network domain is isolated, making it impossible to conduct correlation analysis of end-to-end traffic paths [RFC9312].

2.4. Insufficient In-Depth Analysis

For instance, the IPv6 transformation in some private network applications is not thorough enough, with internal application systems yet to be upgraded. This results in secondary and tertiary links, as well as multimedia content traffic, still relying predominantly on IPv4. However, there is a lack of effective deep monitoring methods to oversee these connections.

2.5. Limited Dynamic Prediction

Existing models find it difficult to quantify the impact of external factors such as policies and regulations, user behavior patterns, and market dynamics on the evolution of IPv6.

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

This system adheres to the following core principles.

* Correlation analysis: Capabilities for cross-domain data integration and analysis

* Business orientation: A standardized indicator measurement system

* Visualized operation: Key operations supported by visual charts

* Scalability: Full utilization of current infrastructure, support for external system docking, and compatibility with multi-vendor devices and subsystems

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

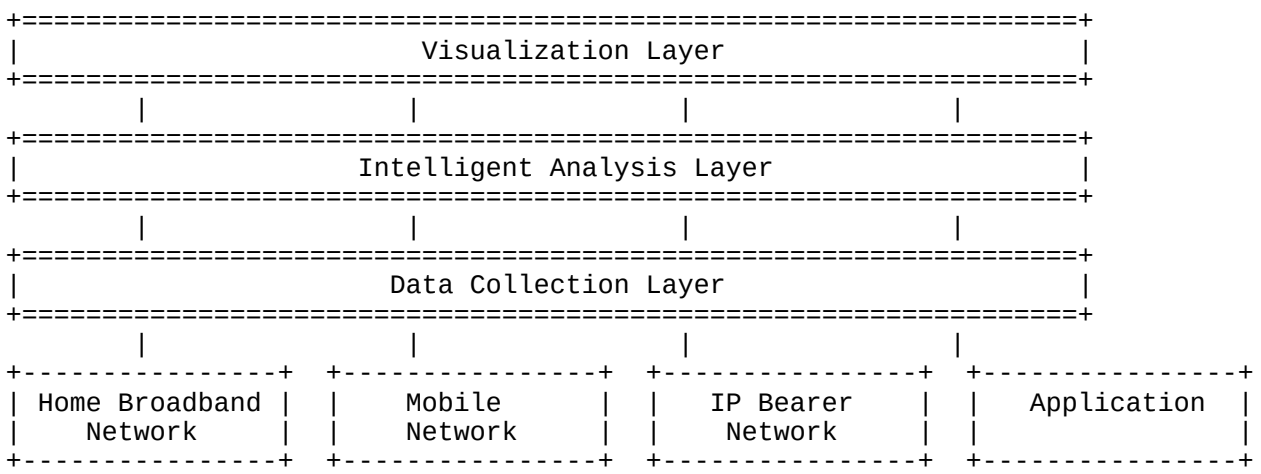

Figure 1: IPv6 Network End to End Monitoring and Analysis System

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.

Based on network functions and service scenarios, the network is divided into four major professional network domains. These specifically include: Home Broadband Network, Mobile Network, IP Bearer Network, and Application.

3.1.1. Data Collection Layer

For these four major professional network domains, data cleaning, transformation, and standardization are performed respectively. Based on multi-source data fusion methods, the aggregation, correlation and integration of data from each professional network are realized, forming a unified data analysis foundation. According to the hierarchical division of the network architecture, the collected data indicators are explained from three dimensions: the

user side, the network side and the application side. The core collection indicators are specified as follows. For specific indicator details, refer to Section 3.2.

* User side: network element readiness, network readiness, basic resources, network traffic, active connections.

* Network side: network element readiness, network readiness, basic resources, network traffic, active connections.

* Application side: network element readiness, network readiness, basic resources, network traffic, active connections. 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.

TBD.

3.1.2. Intelligent Analysis Layer

The system develops a fine-grained, multi-dimensional traffic analysis model. It enables correlated analysis of monitoring data from cloud, network, edge, and end systems. This allows accurate identification of issues related to IPv6 traffic improvement.

3.1.2.1. Multi-domain Traffic Correlation Analysis

* End-to-end cross-system integration: Integrate end-to-end data from professional systems such as user home networks, access networks, metro networks, IDCs, and content providers (covering cloud, network, edge, and end). This enables end-to-end traffic analysis, quality localization and demarcation, and evaluation of overall IPv6 support.

* End-to-end traffic analysis: Perform correlated analysis on traffic data from end, network, and cloud systems. It precisely attributes the causes of IPv6 traffic changes to end, network, or cloud subsystems.

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

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

- Inter-network traffic analysis: Support analysis of IPv6/IPv4 traffic direction and application bearing information between municipal-level networks. Provide an inter-municipal traffic matrix.

* Dynamic traffic attribution

- Identify traffic-restricted areas. Develop multi-dimensional problem investigation plans covering the network side, user side, and application side. Investigate potential influencing factors level by level. Attribute traffic fluctuations to specific subsystems.

3.1.2.2. Quality Deterioration Delimitation and Topology Restoration

* User-level Topology Reconstruction: Using user services as the link, reconstruct the end-to-end topology and diagnose latency/ packet loss segment by segment (e.g., segmental quality of home terminal, access network, and application sides).

* Segmented Quality Degradation Localization: Compare IPv4/IPv6 performance differences segment by segment to locate degraded network elements.

3.1.3. Visualization Layer

3.1.3.1. Indicator-Based Presentation

Data is statistically aggregated and presented according to scenarios, with support for manual editing of display content and dimensions.

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.

* 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

When User A experiences network congestion while playing cloud-based games at home, it affects the gaming experience. To identify the cause, it is necessary to collect performance data from each network segment for quality localization. However, current independent management of network domains prevents direct data correlation. The network segments are as follows: N1 (terminal device to ONT), N2 (ONT to BRAS), and N3 (BRAS to application side).

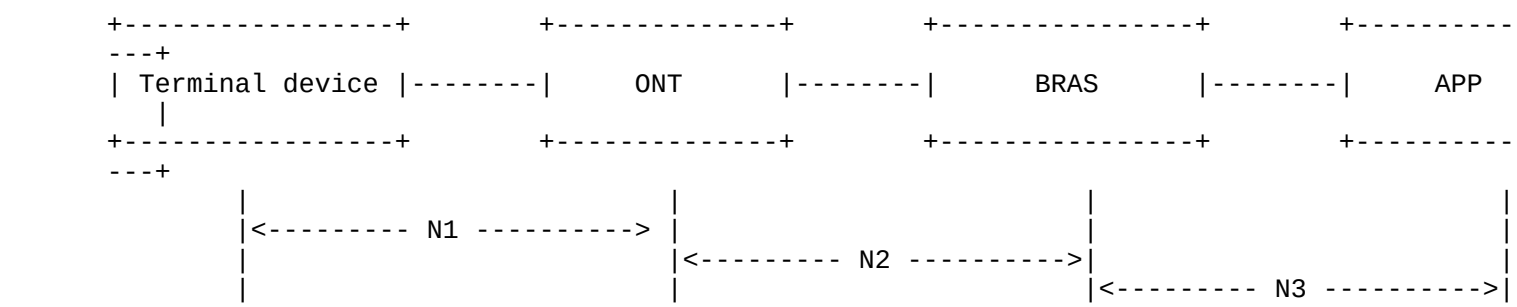

Figure 2: Network schematic diagram based on home broadband network access application

The system detected end-to-end quality degradation of a certain service. After the system segmented and delimited the quality degradation, it compared the performance of N1/N2/N3 segment by segment based on its preset multi-segment monitoring model (Figure 2). It was determined that an abnormality occurred in the N3 network segment. At the same time, by correlating with CDN scheduling logs, a content source switching event was found. The original service node was a local IDC, while the monitored service node was a remote node across provinces. Therefore, it is concluded that the end-to-end quality degradation is caused by CDN remote scheduling and the bottleneck of the N3 cross-network link. Adjusting the CDN scheduling strategy can improve the quality degradation issue.

5.2. Home terminals and router Traffic Analysis

Home terminals and routers, as the "last kilometer" for users to access the Internet, play a crucial role in user experience with regard to their IPv6 support. The system detected that the proportion of IPv6 traffic in a demonstration community was lower than the city-wide average. By correlating with home broadband terminal data, it was found that the proportion of bridge-mode optical modems in this community was relatively high, and the proportion of old devices among the connected routers was higher than the average. Therefore, the root cause was identified as inadequate terminal support. Old routers only support IPv4/NAT mode, which forces IPv6 traffic to be downgraded. Targeted terminal replacements were carried out. Specifically, bridge-mode optical modems for community users were upgraded to router-mode ones. This has led to a significant increase in the proportion of IPv6 traffic.

6. 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.

7. IANA Considerations

TBD.

8. References

8.1. 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>.

8.2. 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