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

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

19 November 2025

IPv6 Network Deployment Monitoring and Analysis
draft-pang-v6ops-ipv6-monitoring-deployment-04

Abstract

This document identifies 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 enable 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 23 May 2026.

Copyright Notice

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 has been accelerating over the past years, the IPv6 protocol was elevated to an Internet Standard status [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 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 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. IPv6 Network End-to-End Monitoring and Analysis Architecture

To overcome the above challenges, the document describes an architecture for IPv6 network end-to-end monitoring and analysis. The architecture is designed to provide comprehensive visibility into IPv6 deployment while maintaining interoperability and scalability.

3.1. Architectural Principles

The monitoring framework is designed around the following key principles:

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

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

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

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

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

* Extensibility: Support integration with existing monitoring infrastructure while allowing for future enhancements.

3.2. Architecture Components

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

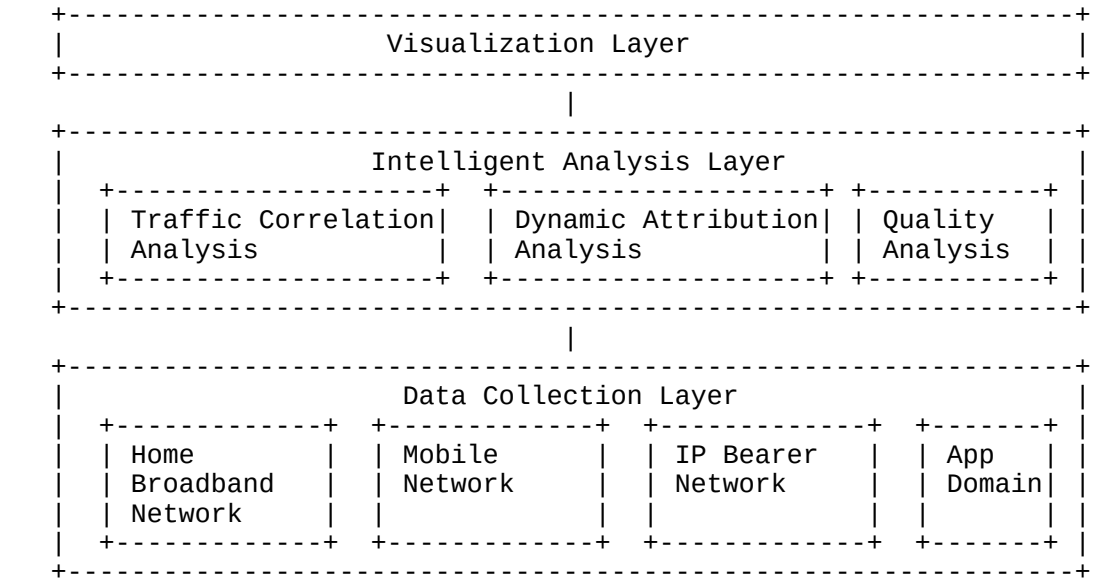

Figure 1: IPv6 Network End-to-End Monitoring and Analysis Architecture

3.2.1. Data Collection Layer

Defines unified interface standards to integrate multi-source data from home broadband network, mobile network, IP bearer network and application. The framework is designed to integrate with multi-vendor devices and subsystems.

Implementations are encouraged to leverage existing IETF standards for data collection where available.

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

* Adopt established standardized data collection mechanisms (such as Telemetry, NETCONF/YANG, etc.) to ensure uniformity of data formats to meet second-level/minute-level traffic monitoring requirements.

3.2.2. Intelligent Analysis Layer

The Intelligent Analysis Layer processes the traffic data collected from the four major professional domains. By employing multi-dimensional traffic analysis models and a set of key indicators, it enables granular insights and facilitates cross-domain root cause diagnosis. This layer also supports certain AI-based model extensions.

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. Analyze traffic change trends.

* User Side traffic analysis: Monitors devices and access networks on the user side (including fixed and mobile networks), supporting IPv6 capability monitoring for home optical network terminals (ONTs), connected routers, end-user devices, and access networks.

* Application traffic analysis: Supports collection and analysis of IPv6/IPv4 active applications on the 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.

3.2.2.2. Dynamic traffic attribution

Based on network traffic analysis results from each professional domain, this component identifies regions with high IPv4 legacy traffic. Using multi-domain traffic correlation analysis results, it attributes traffic fluctuations to specific subsystems.

Optionally, solutions for issues in subsystems can be implemented by combining with other mechanisms such as Happy Eyeballs.

3.2.2.3. Traffic Quality Analysis

* 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).

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

* IPv6 Application Access Quality Assessment: Evaluates key performance indicators of application systems in IPv6 environments from a network performance perspective, including response time, connection success rate, and data transmission rate.

3.2.3. Visualization Layer

The visualization layer presents analyzed data through operational interfaces designed to support network management decisions.

Key presentation capabilities include:

* Unified Operational Dashboard: Presents a overview of key IPv6 deployment metrics and ecosystem trends through real-time summary cards, charts, graphs, and other visual elements.

* Cross-Domain Topology Views: Renders interactive topology maps for each professional network domain, visually representing the state of IPv6-enabled resources, their connections, and operational status based on data from the analysis layer.

* Multi-Dimensional Data Exploration: Provides various chart-based views (e.g., traffic distribution graphs, quality trend lines, comparative application support charts, etc.) that allow operators to filter and examine the indicator data by dimensions such as time, region, service type, and more.

* Fault and Status Visualization: Translates root cause analysis results from the underlying layer into visual cues on dashboards and topology maps, such as color-coded node alerts, geographic heat maps, and other indicators, to accelerate problem recognition and navigation to relevant details.

3.2.4. Indicator System

A comprehensive indicator system for IPv6 support monitoring and analysis includes the following categories:

* 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, Dedicated Lines, and Data Center Network (DCN) Infrastructure.
  - Network Readiness:
    - IPv6 Network Coverage of Backbone Networks, Metropolitan Area Networks (MANs), Internet Data Centers (IDCs), and Dedicated Lines.
    - End-to-End IPv6 Network Performance of Backbone Networks, Metropolitan Area Networks (MANs), Internet Data Centers (IDCs), Dedicated 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), Dedicated Lines, and Applications.
  - Active IPv6 Connections: Active IPv6 Connection Share in Fixed Metropolitan Area Networks (MANs), Mobile Core Networks, Internet Data Centers (IDCs), Dedicated Lines, and Applications.

* Quality Metrics
  - DNS Resolution Performance
  - End-to-End Latency
  - Packet Loss Ratio
* Policy Compliance Indicators

4. Implementation Considerations

This practice has been deployed in operational networks, leading to measurable improvements in IPv6 deployment. Based on deployment experience in major operator networks, we summarize the following key implementation recommendations:

4.1. 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.

4.2. Organizational Collaboration Model

* Establish cross-departmental (fixed, mobile, IP bearer, application, etc.) joint teams to ensure data sharing and process integration.
* Define data management responsibility for each domain and establish data quality governance mechanisms.

4.3. 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.

5. Security Considerations

Implementations are expected to provide: * Role-based access control. * Anonymization of user-specific data. * Secure data transmission protocols. * Integrity verification for collected metrics.

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>.

[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