

nmop
Internet-Draft
Intended status: Standards Track
Expires: 9 May 2026

R. Pang, Ed.
J. Zhao, Ed.
S. Zhang, Ed.
W. Lv, Ed.
H. Wang, Ed.
China Unicom
5 November 2025

Knowledge Graph for Network Traffic Monitoring and Analysis
draft-pang-nmop-kg-for-traffic-monitoring-analysis-02

Abstract

This document extends the knowledge graph framework specifically to the traffic management domain, demonstrating how knowledge graphs can address long-standing traffic management challenges through semantic integration and automated reasoning.

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 9 May 2026.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
2. Network Traffic Monitoring and Analysis System	2
2.1. Multi-Domain Network Environment	3
2.2. Requirements for Unified Monitoring and Analysis	4
3. Knowledge Graph Applications in Traffic Monitoring and Analysis	4
4. Knowledge Graph Implementation Considerations	5
5. Security Considerations	5
6. IANA Considerations	5
7. Informative References	5
Authors' Addresses	6

1. Introduction

Network traffic monitoring and analysis are crucial for ensuring service quality, detecting anomalies, and optimizing network performance. However, modern networks face increasingly severe challenges in managing traffic data from different sources, each with its own formats and schemas. These challenges align with broader operational issues identified in [I-D.mackey-nmop-kg-for-netops], such as data silos, loss of context, and complex correlation requirements.

This document extends the knowledge graph framework specifically to the traffic management domain, demonstrating how knowledge graphs can address long-standing traffic management challenges through semantic integration and automated reasoning.

2. Network Traffic Monitoring and Analysis System

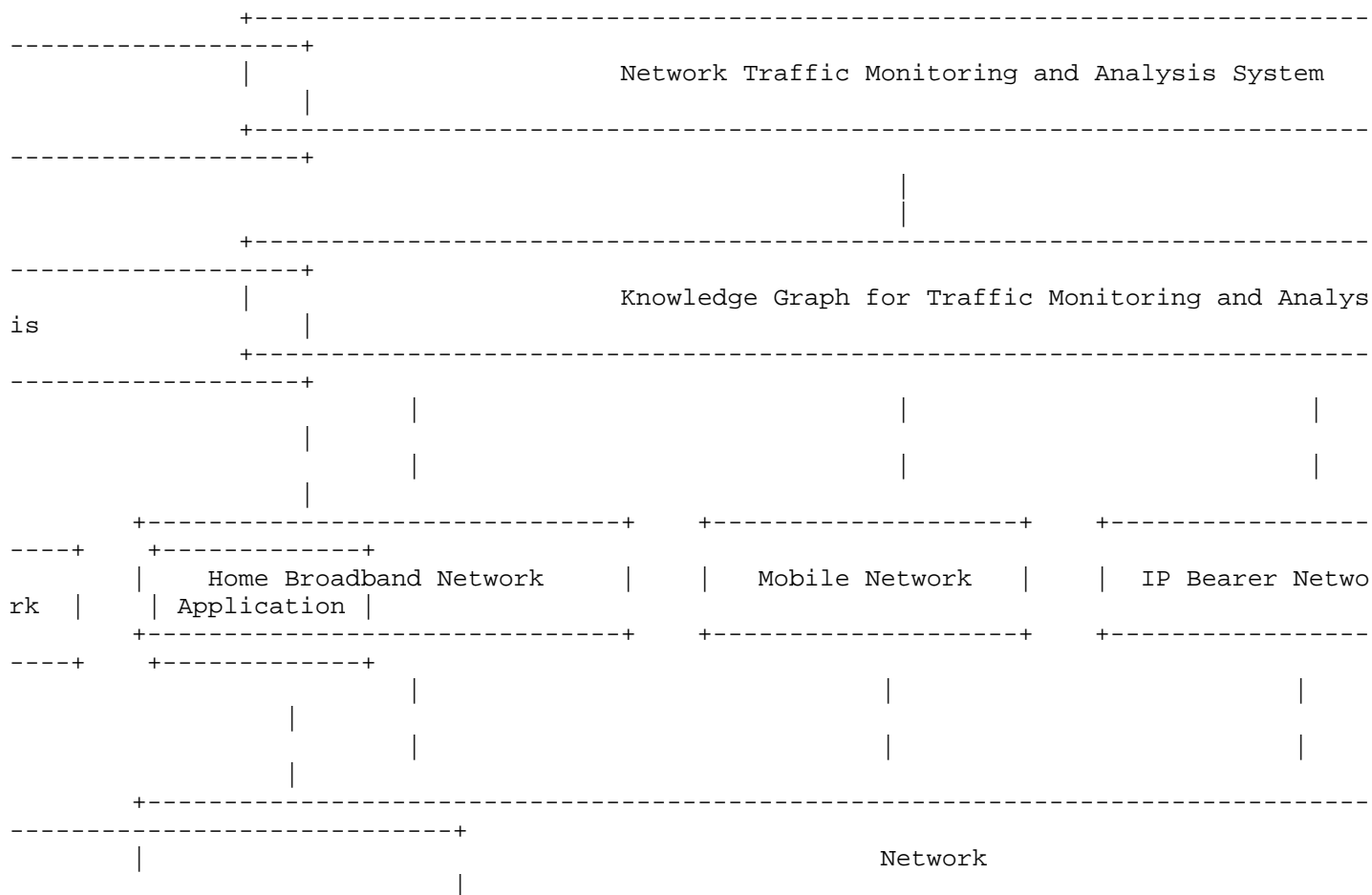
2.1. Multi-Domain Network Environment

Operators' networks typically consist of multiple domains, such as home broadband, mobile, IP bearer, and application networks. These domains interconnect to form diverse end-to-end communication paths; however, data from each domain is managed by independent systems, leading to heterogeneous formats and semantic inconsistencies that create data silos.

A Network Traffic Monitoring and Analysis System is therefore essential to correlate data across these domains and deliver the following functionalities:

- * End-to-End Quality Degradation Identification: Detect and localize quality issues across concatenated network domains.
- * Internet Traffic Flow Analysis: Trace and analyze traffic flow patterns and directions through the network infrastructure.
- * Performance Optimization through Reasoning: Enable network performance optimization through knowledge-based inference.
- * CDN Optimization Support: Facilitate content delivery network layout optimization through rule-based inference mechanisms.

The core challenge stems from service traffic traversing multiple domains. Although inherent relationships exist between the distributed data sources, a single network event is often captured using different dimensions and terminologies across separate systems.



+-----+
-----+

Figure 1: Network Traffic Monitoring and Analysis System Architecture

2.2. Requirements for Unified Monitoring and Analysis

To achieve its intended functionalities, the system necessitates a semantic framework capable of unifying disparate data sources while preserving domain-specific context and enabling cross-domain correlation.

YANG models provide standardized data definitions for individual domains, but their cross-domain application poses significant challenges. Discrepancies between models and the use of disparate terminology hinder the establishment of logical relationships. Additionally, the natural inflexibility of their static tree structure is ill-suited for representing complex network dependencies. Most importantly, this inflexibility impedes automated association and reasoning.

These limitations correspond precisely to the problems that knowledge graphs are designed to address. The knowledge graph framework for network operations [I-D.mackey-nmop-kg-for-netops], based on semantic web technologies, provides a structured approach to integrating, correlating, and reasoning over heterogeneous data. By applying knowledge graph technology, operators can implement comprehensive network traffic monitoring and analysis systems that overcome these cross-domain integration challenges.

TBD.

3. Knowledge Graph Applications in Traffic Monitoring and Analysis

To enable comprehensive monitoring and analysis of overall network status, operators require a unified semantic representation framework that bridges data barriers across network domains.

Knowledge graph technology can construct a unified ontology model to semantically align and associate network entities, events, and their relationships, thereby enabling global knowledge integration of network data.

The integration of a knowledge graph fundamentally transforms conventional network monitoring and analysis systems into a Knowledge-Based System (KBS) architecture. This transformation centers on two core components: the knowledge base and the inference engine, which work in tandem to overcome traditional limitations in traffic analysis.

This KBS architecture effectively transforms fragmented data sources into an intelligent system capable of semantic reasoning and automated analysis, significantly enhancing the efficiency and effectiveness of network traffic monitoring and management operations.

TBD.

4. Knowledge Graph Implementation Considerations

Several approaches exist for constructing the knowledge base for network traffic monitoring:

- * FAIR Principles-Based Construction: Knowledge graphs are constructed using the Semantic Web technology stack. Further details on knowledge graph construction methodologies can be found in [I-D.marcas-nmop-kg-construct].
- * YANG Model Conversion: Transforming YANG models into knowledge graph representations, maintaining compatibility with existing management systems while enabling semantic technology benefits. This approach leverages existing standardization efforts while extending them with semantic capabilities.

* Additional Approaches

TBD.

5. Security Considerations

TBD.

6. IANA Considerations

TBD.

7. Informative References

[I-D.mackey-nmop-kg-for-netops]
Mackey, M., Claise, B., Graf, T., Keller, H., Voyer, D., Lucente, P., and I. D. Martinez-Casanueva, "Knowledge Graph Framework for Network Operations", Work in Progress, Internet-Draft, draft-mackey-nmop-kg-for-netops-03, 2 September 2025, <<https://datatracker.ietf.org/doc/html/draft-mackey-nmop-kg-for-netops-03>>.

[I-D.marcas-nmop-kg-construct]

Martinez-Casanueva, I. D., Rodríguez, L. C., and P.
Martinez-Julia, "Knowledge Graph Construction from Network
Data Sources", Work in Progress, Internet-Draft, draft-
marcas-nmop-kg-construct-00, 26 February 2025,
<<https://datatracker.ietf.org/doc/html/draft-marcas-nmop-kg-construct-00>>.

Authors' Addresses

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

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

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

Wenxiang Lv (editor)
China Unicom
Beijing
China
Email: lvwx28@chinaunicom.cn

Hongyu Wang (editor)
China Unicom
Beijing
China
Email: wanghy3858@chinaunicom.cn