idr
Internet-Draft
Intended status: Standards Track
Expires: 8 January 2026

R. Pang, Ed.
J. Zhao, Ed.
S. Zhang, Ed.
China Unicom

7 July 2025

Knowledge Graph for Network Traffic Monitoring and Analysis
draft-pang-nmop-kg-for-traffic-monitoring-analysis-00

Abstract

This document extends the knowledge graph framework to the field of traffic monitoring, 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 8 January 2026.

Table of Contents

1. Introduction 2
2. Problem Statement 2
3. Formal Ontology Design 3
3.1. Core Classes and Relationships 3
4. Knowledge Graph Construction Pipeline 3
4.1. Ingestion 3
4.2. Mapping 4
4.3. Integration 4
5. Inference Engine and Policy Generation 4
5.1. SPARQL Cross-Scenario Query 4
5.2. Dynamic Policy Execution and Verification (SHACL Constraints) 5
6. Conformance with FAIR Principles 5
7. Future Dynamic Maintenance Mechanism 6
8. Application Scenario Examples 6
9. Security Considerations 6
10. IANA Considerations 6
11. Informative References 6
Authors' Addresses 7

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.

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

2. Problem Statement

There are pain points in traffic monitoring and analysis, such as complex cross-domain correlations and inefficient root-cause analysis. Therefore, the traffic monitoring system can serve as an input source for the knowledge engine to build a semantic network digital twin, mapping the physical network into a virtual knowledge graph and enabling closed-loop decision-making based on the inference

engine.

3. Formal Ontology Design

3.1. Core Classes and Relationships

Class	Definition	Key Subclasses	Critical Relationships
MonitoringObject	Entities observed in traffic monitoring (network components, terminals, apps).	NetworkElement (routers, switches), Terminal (phones, ONTs), Application	* isMonitoredBy (to DataSource), * hasMetric (to MonitoringMetric)
DataSource	Systems/tools collecting traffic data.	NetflowCollector, Probe, ISPNetworkManager(interface designed by YANG models)	* providesDataTo (to AnalysisScenario), * collectsFrom (to MonitoringObject)
MonitoringMetric	Quantifiable indicators of traffic characteristics.	NetworkElementReadiness, ApplicationReadiness, NetworkReadiness, CloudReadiness, ActiveConnections, IPv6Traffic	* measures (to MonitoringObject/to AnalysisScenario), * hasThreshold (to numerical value)
AnalysisDimension	Perspectives for traffic analysis.	NetworkSideAnalysis(NetworkTrafficAnalysis, InterNetworkAnalysis), UserSideAnalysis, ApplicationSideAnalysis, TrafficQualityAnalysis	* isUsedIn (to AnalysisScenario), * includesMetric (to MonitoringMetric)
AnalysisScenario	Business-specific analysis scenarios.	HomeBroadbandAnalysis, MobileNetworkAnalysis, IPBearer NetwokAnalysis, ApplicationAnalysis	* coversObject (to MonitoringObject), * usesDimension (to AnalysisDimension)
Policy	Automated rules triggered by metrics or scenarios.	TrafficLimitingPolicy, TerminalUpgradePolicy QualityOptimizationPolicy	* isTriggeredBy (to MonitoringMetric), * appliesTo (to MonitoringObject)

The MonitoringMetric refers to the indicator system in [I-D.pang-v6ops-ipv6-monitoring-deployment].
TBD.

4. Knowledge Graph Construction Pipeline

Following the ETL-based approach in [I-D.marcas-nmop-kg-construct],

the pipeline for traffic monitoring KG includes three stages:

4.1. Ingestion

Extract home broadband data from the ISP network management system, including:
* Terminal data: Home router model, IPv6 support status (NetworkElementReadiness). * Traffic data: Daily IPv6 traffic ratio (IPv6TrafficRatio).

4.2. Mapping

Convert raw data into knowledge graph triples using RDF mapping languages, with examples:

```
 @prefix ont: <http://trafficmonitoring/ontology#> .
  //Home router (terminal entity)
   <Router/Home-001> a ont:Terminal;
   ont:hasModel "HR-200";
   ont:NetworkElementReadiness "IPv6 unsupported".

  //IPv6 traffic metric (linked to analysis scenario)
   <Metric/IPv6/Home-001> a ont:IPv6Traffic;
   ont:value "6%";
   ont:isUsedIn <Scenario/HomeBroadbandAnalysis>.

 // Scenario-terminal association
   <Scenario/HomeBroadbandAnalysis> ont:coversObject <Router/Home-001> .
```

4.3. Integration

Construct a unified view through semantic associations: Link identical terminals across systems using owl:sameAs (e.g., MAC address and device ID); Establish "terminal-metric-scenario" association chains to enable cross-dimensional analysis.

5. Inference Engine and Policy Generation

Rule-Based Reasoning

If "home router NetworkElementReadiness=IPv6 unsupported" and "IPv6TrafficRatio<10% in HomeBroadbandAnalysis scenario", then trigger TerminalUpgradePolicy.

5.1. SPARQL Cross-Scenario Query

Query "all scenarios where the IPv6 traffic proportion < 10% and the associated terminals":

```
PREFIX ont: <http://trafficmonitoring/ontology#>
SELECT ?scenario ?terminalModel
WHERE {
 ?scenario a ont:AnalysisScenario .
 ?scenario ont:coversObject ?terminal .
 ?terminal a ont:Terminal .
 ?terminal ont:hasModel ?terminalModel .
 ?terminal ont:hasMetric ?metric .
 ?metric a ont:IPv6Traffic .
 ?metric ont:value ?metricValue .
 FILTER (xsd:decimal(?metricValue) < 10)
}
```

5.2. Dynamic Policy Execution and Verification (SHACL Constraints)

Define policy execution conditions through SHACL to ensure the legality of rules:
Constraints for the terminal upgrade policy: It takes effect only when the terminal support rate < 30% and the scenario is home broadband.

```
ont:TerminalUpgradeShape a sh:NodeShape ;
  sh:targetClass ont:TerminalUpgradePolicy ;
  sh:property [
    sh:path ont:appliesTo ;
    sh:class ont:Terminal
  ] ;
  sh:property [
    sh:path ont:triggeredBy ;
    sh:property [
      sh:path ont:NetworkElementReadiness ;
      sh:lessThan 30 ;
      sh:datatype xsd:integer
     ] ;
     sh:property [
     sh:path ont:AnalysisScenario ;
     sh:hasValue ont:HomeBroadband
     ]
     ] .
```

6. Conformance with FAIR Principles

* Findability: Each class and instance is assigned a unique URI (e.g., http://trafficmonitoring/object/ONT10086).

* Interoperability: Cross-system mapping of metrics and dimensions is achieved through attributes such as belongsToDimension.

* Reusability: Sub-categories of AnalysisDimension (such as "traffic quality analysis") can be reused in multiple scenarios such as home broadband and mobile networks.

7. Future Dynamic Maintenance Mechanism

* Supports knowledge evolution. Telemetry data can be real-time converted into RDF triples.

* Incremental expansion mechanism.

* Automatically expands the ontology structure when a new network domain is added.

* Adaptive optimization. Dynamically adjusts rule thresholds based on historical data analysis. TBD.

8. Application Scenario Examples

* IPv6 deployment bottleneck analysis

* Metropolitan area network traffic flow direction optimization

* Fault quick positioning

* Traffic anomaly detection.

TBD.

9. Security Considerations

TBD.

10. IANA Considerations

TBD.

11. 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-02, 4 March 2025, <https://datatracker.ietf.org/doc/html/draft-mackey-nmop-kg-for-netops-02>.

[I-D.marcas-nmop-kg-construct]
Martinez-Casanueva, I. D., Rodr鱈guez, 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>.

[I-D.pang-v6ops-ipv6-monitoring-deployment]
Pang, R., Zhao, J., Jin, M., and S. Zhang, "IPv6 Network Deployment Monitoring and Analysis", Work in Progress, Internet-Draft, draft-pang-v6ops-ipv6-monitoring-deployment-01, 4 July 2025, <https://datatracker.ietf.org/doc/html/draft-pang-v6ops-ipv6-monitoring-deployment-01>.

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