

rtgwg
Internet-Draft
Intended status: Informational
Expires: 7 May 2026

R. Zhang
J. Mao
B. Liu
N. Geng
X. Shang
Q. Gao
Z. Li
Huawei
3 November 2025

Use Cases and Requirements of Communication Protocol for Measurement
Agents on Network Devices
draft-zhang-rtgwg-ai-agents-measurement-00

Abstract

This document focuses on the use cases and requirements of communication protocols for measurement agents on network devices.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at <https://example.com/LATEST>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-zhang-rtgwg-ai-agents-measurement/>.

Discussion of this document takes place on the rtgwg Working Group mailing list (<mailto:WG@example.com>), which is archived at <https://example.com/WG>.

Source for this draft and an issue tracker can be found at <https://github.com/USER/REPO>.

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 7 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	3
2. Conventions and Definitions	3
3. Use Cases	3
3.1. Use Case 1: Latency Measurement	3
3.2. Use Case 2: Active Measurement	4
4. Requirements	4
4.1. Transmission	4
4.2. Data Formats	5
4.3. Security	5
4.4. Reliability	5
4.5. Scalability	5
4.6. Interoperability	6
5. Security Considerations	6
6. IANA Considerations	6
7. Conclusion	6
8. Normative References	6
Acknowledgments	6
Authors' Addresses	6

1. Introduction

This document outlines use cases and requirements for network device agents engaged in network measurement tasks. As networks evolve toward increased automation and intelligence, efficient and standardized interactions between agents (located in routers, switches, or other network elements) become critical. Network measurement supports scientific discovery and network operations through tasks like characterizing traffic, understanding protocol performance, billing customers and detecting problems. This draft focuses on defining use cases that illustrate practical communication flows between agents, utilizing protocols like HTTP, gRPC, and others, and establishes key requirements to ensure interoperability, scalability, and reliability. The methods of measurement is out of scope in this draft. But the measurement agents on network devices should have the ability of choosing and invoking suitable network measurement tool.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Use Cases

This section describes three use cases for communication between network device agents for network measurement. Each case follows the follow:

1. Intent analysis
2. Measurement configuration generation
3. Configuration deployment

3.1. Use Case 1: Latency Measurement

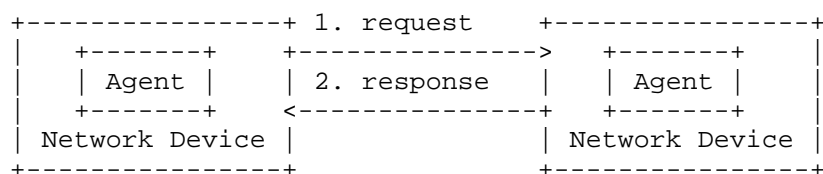


Figure: Latency Measurement

In this scenario, an agent analyzes network performance intent and generates a latency measurement configuration. The intent may generate by other agent or human. The configuration specifies ICMP-based measurement with a 5-second duration. The agent sends an HTTP GET request to related agent's endpoint with the configuration parameters. The agent which receives this request applies the configuration, executes the measurement, and returns results in JSON format containing average latency, jitter, and timestamps.

Overall, this approach promotes interoperability and ease of integration in heterogeneous networks.

3.2. Use Case 2: Active Measurement

This use case involves an agent perceived or received a risk of link congestion initiates an active probing measurement. The agent should analyzes the level of risk to determine probe type and frequency. After analyzing the agent generates a configuration specifying active probing. There may be multiple related agent to cooperate to handle this issue. When probe arriving destinations, related agents should send reports to the agent on the source node.

4. Requirements

To enable effective network measurement between network device agents, several key requirements must be addressed to ensure robust, scalable, and interoperable communications. These requirements stem from the use cases described and broader industry needs, focusing on protocol capabilities, data handling, and system integration.

4.1. Transmission

Support for stream-oriented transmission is essential. As demonstrated in above use cases, measurements often involve continuous data flows, such as real-time metrics or large datasets. Protocols must facilitate bidirectional streaming to allow agents to send and receive data concurrently without interruption, minimizing latency and enabling dynamic adjustments during measurements. This requirement aligns with protocols like gRPC and WebSocket, which natively support streaming, and should be extended to other implementations through standards like HTTP/2 for broader adoption.

4.2. Data Formats

Structured and extensible data formats are critical for interoperability. Agents must exchange measurement results in a consistent manner, using formats such as JSON, XML, or Protocol Buffers. These formats enable easy parsing, validation, and integration with analytics tools. Additionally, the data schema should be extensible to accommodate new measurement types and parameters, allowing for future enhancements without breaking backward compatibility. For instance, defining common fields for timestamps, error codes, and metadata in responses can standardize interactions across diverse agent implementations.

4.3. Security

Security mechanisms must be integrated to protect measurement data and prevent unauthorized access. This includes mandatory use of transport-layer security (e.g., TLS for HTTP and gRPC, WSS for WebSocket) to encrypt data in transit, as well as authentication and authorization frameworks such as OAuth or client certificates. Given the sensitive nature of network metrics, agents should also implement rate limiting and audit logging to detect and mitigate potential threats, ensuring compliance with organizational policies.

4.4. Reliability

Reliability and error handling are paramount for maintaining measurement accuracy. Protocols should incorporate features like retransmission policies, timeouts, and graceful degradation to handle network failures or agent unavailability. For example, in the latency measurement use case, HTTP retries can be employed for transient errors, while gRPC's built-in error codes provide detailed diagnostics. Agents must also support idempotent operations to avoid duplicate measurements and ensure data consistency.

4.5. Scalability

Scalability and performance optimizations are necessary to support large-scale deployments. This involves efficient resource management, such as connection pooling and load balancing, to handle high volumes of concurrent measurements. Protocols should minimize overhead through compression techniques and efficient serialization, as seen with Protocol Buffers in gRPC. Moreover, agents ought to support asynchronous operations to non-blockingly process multiple requests, enhancing overall system throughput.

4.6. Interoperability

Interoperability and standardization across vendor implementations are crucial. This requires adherence to common APIs, protocol specifications, and data models, possibly defined in IETF RFCs. By promoting a unified approach, agents from different manufacturers can seamlessly communicate, reducing integration costs and fostering innovation in network automation. Additional considerations include support for multicast or publish-subscribe models for group measurements and mechanisms for data aggregation to reduce network load.

5. Security Considerations

TBD

6. IANA Considerations

This document has no IANA actions.

7. Conclusion

This draft presents use cases and requirements for the measurement agents on the network device. The defined requirements for transmission, data formats, security, reliability, scalability, and interoperability form a foundation for standardized agent interactions. These improvements will enable more automated and intelligent network management, enhancing performance and resilience in modern networks.

8. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/rfc/rfc2119>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/rfc/rfc8174>>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Ruyi Zhang
Huawei
Email: zhangrui8@huawei.com

Jianwei Mao
Huawei
Email: maojianwei@huawei.com

Bing Liu
Huawei
Email: leo.liubing@huawei.com

Nan Geng
Huawei
Email: gengnan@huawei.com

Xiaotong Shang
Huawei
Email: shangxiaotong@huawei.com

Qiangzhou Gao
Huawei
Email: gaoqiangzhou@huawei.com

Zhenbin Li
Huawei
Email: robinli314@163.com