Network Working Group
Internet-Draft
Intended status: Informational
Expires: 6 May 2026

G. Zeng
J. Mao
B. Liu
N. Geng
X. Shang
Q. Gao
Z. Li
Huawei

2 November 2025

MCP-based Network Measurement Framework: Using Model Context Protocol for Intelligent Network Measurement
draft-zm-rtgwg-mcp-network-measurement-01

Abstract

This document proposes a framework for intelligent network measurement using the Model Context Protocol (MCP). By treating network devices as MCP servers, and treating network controllers, management systems, or network devices with LLM capability as MCP clients, this framework enables natural language-driven, AI-assisted network measurement operations. The framework leverages MCP's standardized communication protocol to provide real-time network performance monitoring, intelligent fault diagnosis, topology discovery, and automated measurement workflows. This document describes the architecture, use cases, and security considerations for implementing MCP-based network measurement systems.

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 6 May 2026.

Table of Contents

1. Introduction

Traditional network measurement approaches often require specialized tools, complex configurations, and expert knowledge. As networks grow in complexity and scale, there is an increasing need for more intelligent and automated measurement solutions. The Model Context Protocol (MCP) provides a standardized framework for enabling communication between AI systems and external data sources.

This document proposes leveraging MCP to create an intelligent network measurement framework where:

* Network devices (routers, switches, firewalls) act as MCP servers
* Network controllers, management systems, or network devices with LLM capability act as MCP clients
* Natural language queries drive measurement operations
* AI systems assist in analysis and decision-making

The key benefits of this approach include:

* *Natural Language Interface*: Network operators can perform measurements using natural language queries
* *AI-Assisted Analysis*: Intelligent analysis of measurement results and anomaly detection
* *Standardized Communication*: Uniform protocol across different vendor devices
* *Automated Workflows*: Reduced manual intervention in measurement processes

2. Terminology

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. MCP-Based Network Measurement Architecture

3.1. Architectural Components

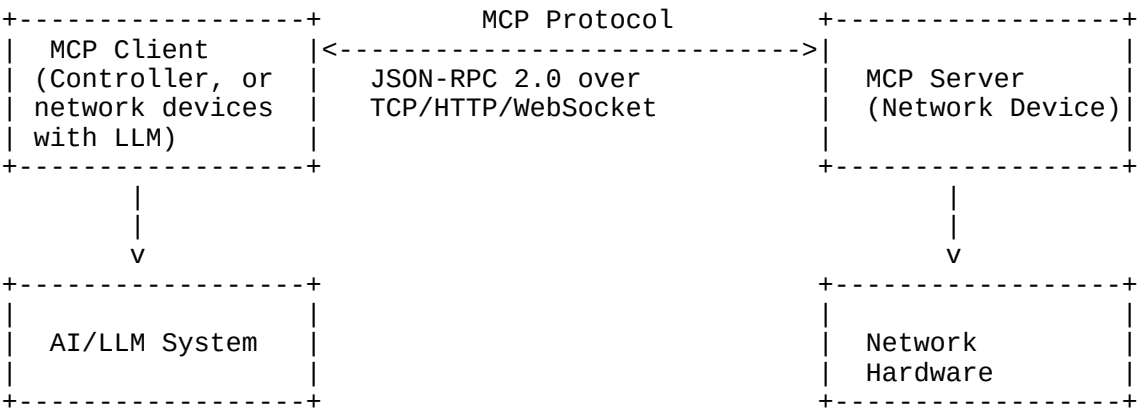

Figure 1: MCP Network Measurement Architecture

3.2. Communication Flow

The communication process involves five phases:

* *Discovery Phase*: MCP client discovers available MCP servers and their capabilities

* *Capability Negotiation*: Client and server negotiate supported measurement features

* *Measurement Execution*: Client requests measurements using natural language or structured queries

* *Data Collection*: Server provides measurement data through resources or tool execution

* *Analysis and Response*: Client processes results, potentially with AI assistance

3.3. MCP Server Capabilities

MCP servers MUST expose:

Measurement Resources:

* Interface statistics (bandwidth, utilization, errors)

* Routing information (tables, protocols, neighbors)

* Device performance metrics (CPU, memory)

* Network topology data (LLDP/CDP information)

Measurement Tools:

* Connectivity tests (ping, traceroute)

* Performance measurements (throughput, latency)

* Protocol-specific diagnostics

* Configuration validation tools

3.4. MCP Client Capabilities

MCP clients MAY provide:

* *Sampling capabilities*: For complex measurement scenarios

* *Root context*: Measurement scope and boundaries

* *User interaction*: For measurement confirmation and authorization

4. Use Cases

4.1. Real-time Network Performance Monitoring

Scenario: Network operator wants to check link utilization across core routers.

MCP Interaction:

```
Operator: "Show me the current utilization of all core router interfaces"
MCP Client: Discovers core routers and requests interface statistics
MCP Server: Provides Resources containing interface utilization data
MCP Client: Aggregates and presents data with AI-generated insights
```

4.2. Intelligent Fault Diagnosis

Scenario: Troubleshooting connectivity issues between two sites.

MCP Interaction:

```
Operator: "Diagnose connectivity issues between Site A and Site B"
MCP Client: Identifies relevant devices and requests diagnostic tools
MCP Server: Provides Tools: [traceroute, ping, show interfaces, show route]
MCP Client: Executes diagnostic sequence and analyzes results
```

4.3. Network Topology Discovery

Scenario: Automated mapping of network topology.

MCP Interaction:

```
Operator: "Discover and map the current network topology"
MCP Client: Requests topology information from seed devices
MCP Server: Provides Resources: [neighbors table, interface status, VLAN info]
MCP Client: Builds topology graph using AI-assisted correlation
```

4.4. Capacity Planning and Trend Analysis

Scenario: Predict future capacity needs based on current usage patterns.

MCP Interaction:

```
Operator: "Analyze capacity trends for all WAN links"
MCP Client: Collects historical utilization data
MCP Server: Provides Resources: [historical statistics, error counters]
MCP Client: AI analysis generates capacity planning recommendations
```

4.5. Security Incident Response Measurement

Scenario: Measure and analyze potential security threats.

MCP Interaction:

```
Operator: "Investigate unusual traffic patterns on border routers"
MCP Client: Requests security-related measurements
MCP Server: Provides Tools: [ACL hit counts, flow analysis, threat detection]
MCP Client: Correlates security events with network measurements
```

5. Protocol Operations

5.1. Measurement Request Format

Measurement requests MUST follow MCP protocol specifications with the following structure:

```
{
  "jsonrpc": "2.0",
  "method": "tools/call",
  "params": {
    "name": "network_measurement_tool",
    "arguments": {
      "target": "device_or_interface",
      "measurement_type": "ping_throughput_latency",
      "parameters": {
        "count": 10,
        "interval": 1,
        "timeout": 5
      }
    }
  },
  "id": "measurement_request_001"
}
```

5.2. Measurement Response Format

Measurement responses MUST include:

```
{
  "jsonrpc": "2.0",
  "result": {
    "measurement_id": "measurement_request_001",
    "timestamp": "2025-10-18T10:30:00Z",
    "device_id": "router_core_01",
    "results": {
      "avg_latency_ms": 25.3,
      "min_latency_ms": 24.1,
      "max_latency_ms": 28.7,
      "packet_loss_percent": 0.0,
      "throughput_mbps": 987.2
    },
    "metadata": {
      "measurement_duration": 15,
      "path_taken": ["router1", "router2", "router3"]
    }
  },
  "id": "measurement_request_001"
}
```

5.3. Error Handling

MCP servers MUST implement appropriate error handling for:

* Unsupported measurement types

* Device capability limitations

* Resource exhaustion scenarios

* Security policy violations

Error responses MUST follow JSON-RPC 2.0 error format with MCP-specific error codes.

6. Security Considerations

The Model Context Protocol enables powerful capabilities through arbitrary data access and code execution paths. With this power comes important security and trust considerations that all implementers must carefully address.

6.1. Authentication and Authorization

MCP-based network measurement systems MUST implement:

* *Strong Authentication*: All MCP communications MUST be authenticated using industry-standard mechanisms (TLS mutual authentication, OAuth 2.0, etc.)

* *Role-Based Access Control*: Different measurement capabilities MUST be restricted based on user roles and privileges

* *Device Authorization*: Network devices MUST verify client authorization before exposing sensitive measurement data

6.2. Data Privacy and Confidentiality

* *Encryption in Transit*: All MCP communications MUST use TLS 1.3 or higher

* *Data Minimization*: Only necessary measurement data SHOULD be exposed

* *Access Logging*: All measurement requests and responses MUST be logged for audit purposes

6.3. Measurement Tool Security

* *Tool Validation*: All measurement tools exposed by MCP servers MUST be validated for security vulnerabilities

* *Resource Limits*: Measurement tools MUST implement appropriate resource limits to prevent DoS attacks

* *Input Sanitization*: All measurement parameters MUST be validated and sanitized

6.4. AI/LLM Security Considerations

* *Prompt Injection Protection*: Natural language interfaces MUST implement protection against malicious prompt injection

* *Result Sanitization*: Measurement results MUST be sanitized before AI processing

* *Model Security*: AI models used for analysis MUST be protected against adversarial inputs

6.5. Network Device Security

* *Least Privilege*: Network devices MUST expose only necessary measurement capabilities

* *Rate Limiting*: Measurement requests MUST be rate-limited to prevent abuse

* *Network Segmentation*: MCP traffic SHOULD be isolated in management networks

7. IANA Considerations

This document has no IANA actions.

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8259] Bray, T., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, 2017, <https://www.rfc-editor.org/info/rfc8259>.

9. Informative References

[MCP-SPEC] Anthropic, "Model Context Protocol Specification 2025-06-18", URL https://modelcontextprotocol.io/specification/2025-06-18/basic, 2025.

[RFC1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol (SNMP)", RFC 1157, 1990, <https://www.rfc-editor.org/info/rfc1157>.

[RFC3954] Claise, B., "Cisco Systems NetFlow Services Export Version 9", RFC 3954, 2004, <https://www.rfc-editor.org/info/rfc3954>.

Authors' Addresses

Guanming Zeng
Huawei
Email: zengguanming@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