

# Applicability of MCP for the Network Management

draft-yang-nmrg-mcp-nm-02

IETF NMRG Meeting 03/16/2026

on behalf of Authors Team (Yuanyuan Yang, Qin Wu, Diego Lopez, Nathalie Romo Moreno, Lionel Taihardat)

# Recap

- V-00 was presented in IETF 123 NMRG meeting and follow up NMRG interim
- Open issues tracked in the github
  - <https://github.com/Yuanyuan4666/Integration-of-MCP-and-Network-Management-Protocols/issues>
- MCP has seen rapid adoption across both startups and enterprises
  - Use cases such as AI Coding Assistants, database query data analysis tools, etc
- The goal of this document is to explore MCP applicability in the network management
  - High Level Challenges
  - MCP for Network Exposure
  - MCP Discovery
  - Deployment Scenarios
  - Architectural requirements

# The High Level Challenges in adopting MCP in NM

- **Protocol Design**

- Lack entire Error Handling mechanism enforcement
  - Limited to Discovery, Invocation, not applied to Lifecycle management
- Stateful
  - Complicate load balancing, network latency and instability
- Context handling
  - LLM's performance, reason with ambiguity and uncertainty

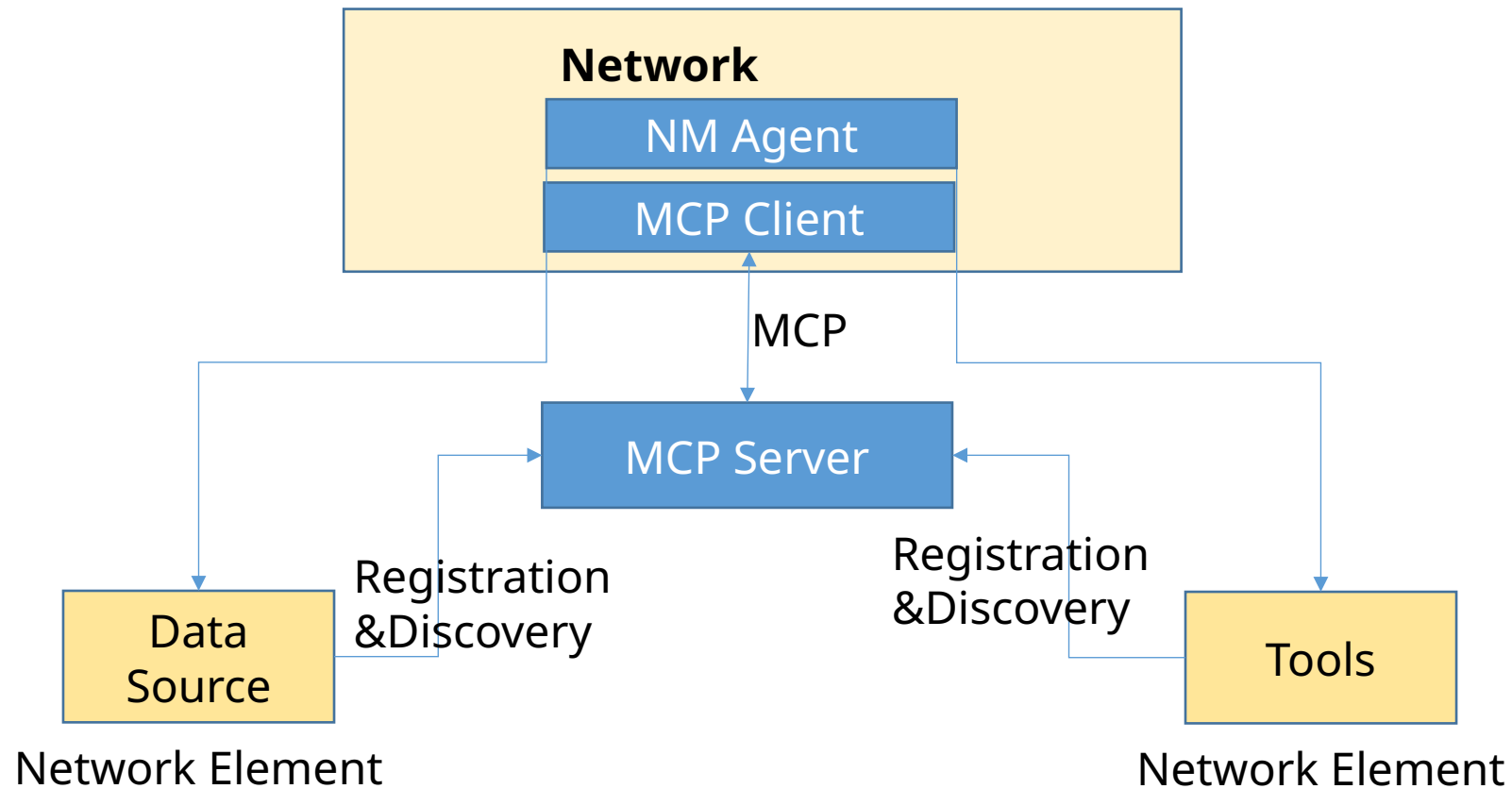
- **Security Consideration**

- Malicious Actors
  - Prompt injection, Tool Poisoning, Tool shadow
- Security Enforcement
  - Rely on external implantations for authentication and authorization
- Identity Management
  - Distinct request from user, agent or shared system account.

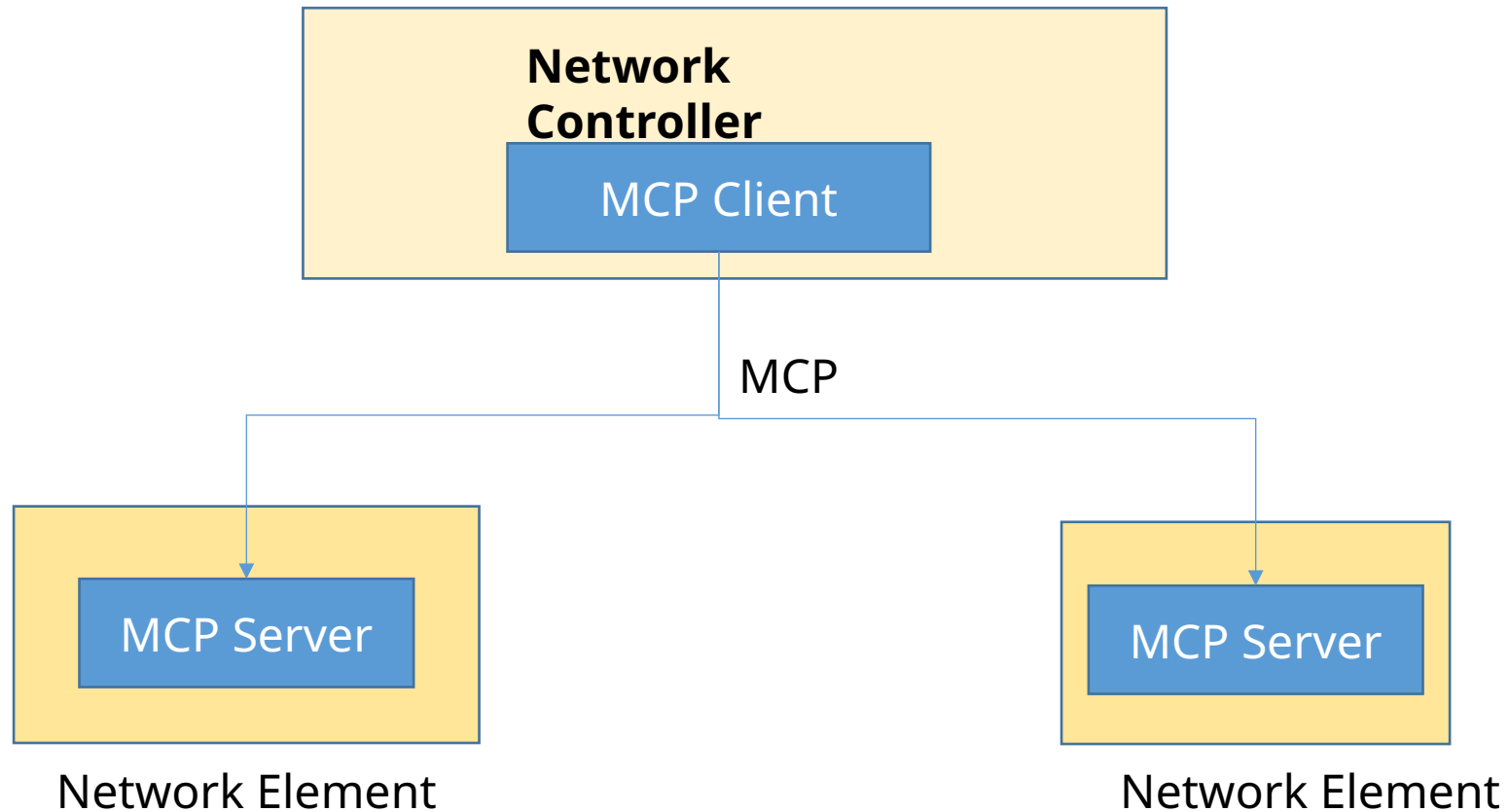
# Deployment Consideration in adopting MCP in the Network Management

- Standalone MCP server to Expose APIs and tools to the Network Controller
- The Network Gateway/Controller and the Network Element Communication using MCP
- Network Element Inter-Communication using MCP
- Network Controller consumes API or Data source using MCP

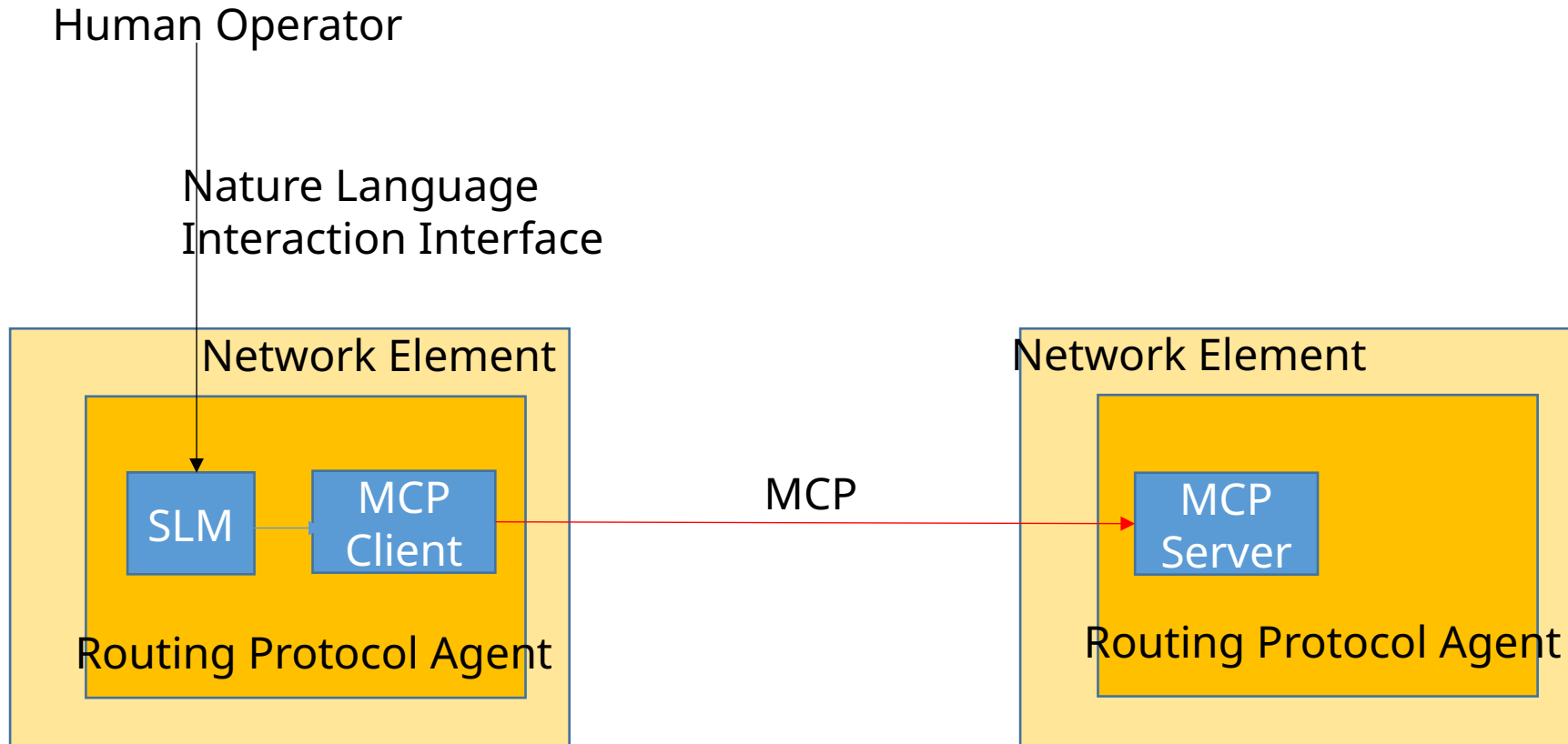
# Standalone MCP server Invoked by Network Controller



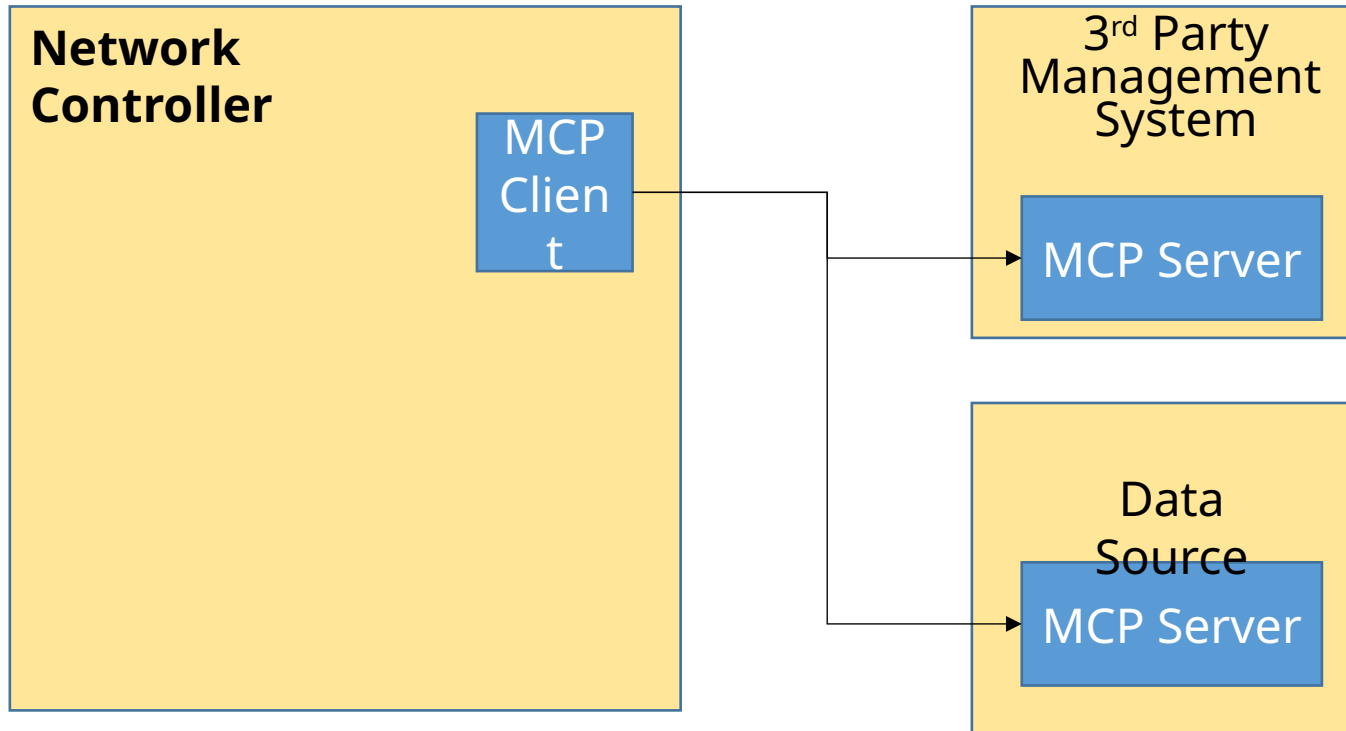
# The Network Gateway/Controller and the Network Element Communication using MCP



# Network Element Inter-Communication using MCP



# Network Controller Consumes API or Data source using MCP



# Key Architectural Requirements

- **Function-Specific MCP Servers:**
  - To maintain proper architecture and performance with growing tool volumes, servers should be categorized by network management functions.
  - Typical categories include network log analysis, device configuration management, energy consumption management, and security operations, etc.
- **Secure and Scalable Architecture:**
  - Enforce strict access controls limiting MCP operations to authorized AI models and users
  - Scale efficiently with increasing number of network devices while maintaining performance
- **Automated Workflows:** MCP implementations should support LLM-coordinated automation of:
  - Real-time diagnostics
  - Fault remediation workflows
  - Other common management operations to reduce operator workload

# Next Step

- Is this work interested to NMRG, Ready for RG Adoption?
- Address issue tickets raised in the GitHub
  - <https://github.com/Yuanyuan4666/Integration-of-MCP-and-Network-Management-Protocols>