

MCP - Introduction

Model Context Protocol (MCP)

What is MCP?

Model Context Protocol (MCP) is an open standard that enables Artificial Intelligence (AI) models, particularly Large Language Models (LLMs), to securely connect with external tools, applications, databases, and data sources. It acts as a common communication layer between AI agents and the systems they need to interact with.

Just as USB provides a standardized way for devices to connect to computers, MCP provides a standardized way for AI models to access external resources and perform actions beyond their built-in capabilities.

Why is MCP Used?

Traditional AI models are limited to the information they were trained on and cannot directly access real-time data or enterprise systems. MCP addresses this limitation by allowing AI applications to:

- Access live and up-to-date information.
- Connect to enterprise tools and business applications.
- Retrieve data from databases and APIs.
- Execute actions through external services.
- Reduce the need for custom integrations for every tool.

By using MCP, organizations can build more powerful and scalable AI solutions without creating separate connectors for each application.

Key Components of MCP

1. MCP Host

The MCP Host is the application that contains or uses the AI model. Examples include AI assistants, chatbots, IDEs, and enterprise AI platforms.

Responsibilities: Initiates requests; Manages communication with MCP servers; Presents results to users.

2. MCP Client

The MCP Client acts as an intermediary between the host and MCP servers.

Responsibilities: Sends requests to MCP servers; Receives responses; Maintains protocol communication.

3. MCP Server

An MCP Server exposes tools, resources, or services that AI models can access. Examples include Database servers, CRM systems, Ticketing platforms, Cloud services, and Internal business applications. The server provides standardized interfaces so that AI models can interact with these systems consistently.

4. Resources

Resources represent data that AI models can read, such as Documents, Database records, Configuration files, and Knowledge bases.

5. Tools

Tools are functions or actions that the AI model can execute, such as creating a support ticket, running a database query, sending an email, or generating a report.

How MCP Works

1. A user submits a request to an AI application.
2. The AI determines that external information or functionality is required.
3. The MCP Client sends a request to an MCP Server.
4. The MCP Server provides access to the required resource or tool.
5. The result is returned to the AI model.
6. The AI generates a response using the retrieved information.

This process enables AI systems to perform tasks that would otherwise be impossible using only their training data.

Benefits of MCP

Standardized Integration: Developers can connect AI models to multiple systems using a common protocol instead of building custom integrations for each application.

Scalability: New tools and services can be added without modifying the AI model itself.

Reusability: The same MCP server can be used by multiple AI applications and agents.

Security: MCP supports controlled access to resources and tools, helping organizations manage permissions and data access.

Improved AI Capabilities: AI models can access real-time data, execute actions, and interact with enterprise systems, making them significantly more useful.

Common Use Cases

- AI-powered customer support systems
- IT service management and ticketing automation
- Enterprise knowledge assistants
- Software development assistants
- Database querying and reporting
- Cloud infrastructure management
- Workflow automation

Conclusion

Model Context Protocol (MCP) is becoming a key standard for connecting AI models with external systems and tools. By providing a unified and secure communication framework, MCP enables AI applications to access real-time information, perform actions, and integrate seamlessly with

enterprise environments. As organizations increasingly adopt AI-driven solutions, MCP plays a crucial role in making AI systems more powerful, scalable, and practical for real-world use.

Revision #2

Created 2026-06-19 06:09:19 UTC by Radesh Chakravarthy

Updated 2026-06-19 06:20:00 UTC by Radesh Chakravarthy