

MCP Communication Flow

Overview

The MCP communication process follows a structured flow from user request to final response, involving all four core components working in sequence.

Step-by-Step Communication Process

1. User Interaction

- User sends prompt/query to host application
- Initial request triggers the MCP workflow

2. Host Processing

- Host application receives user request
- LLM processes and understands the initial query
- Host identifies need for external capabilities

3. Client Connection & Capability Discovery

- Host connects to appropriate MCP server via dedicated client
- Client performs **capability discovery** query to server
- Server returns available capabilities (tools, resources, prompts)
- Information relayed back: Server → Client → Host

4. Capability Invocation

- LLM in host application decides which capabilities to use
- Host sends specific capability requests through client
- Examples: “send email,” “create files,” “fetch data”

5. Server Execution

- Client handles execution call processing
- Server receives and executes requested functions
- Actual task performance occurs at server level

6. Results Integration

- Server returns execution results to client
- Client relays results back to host application
- LLM integrates results into context
- Host generates final response incorporating all executed actions

Communication Flow Summary

User Request → Host Processing → Capability Discovery → Capability Invocation → Server Execution → Results Integration → Final User Response

This flow ensures seamless integration of external capabilities while maintaining security and proper orchestration between all MCP components.