What are MCP agents? Part 1

Facilitator: Alberto Camarena

Presented at: Global Hack Week 🌐 Gen AI

Date: 18/06/25 📅

Agenda

1. What is MCP?
2. Why MCP?
3. Anatomy of MCP
4. Message Types
5. Session & Context Management
6. Tools and Function Calling
7. Building with MCP
8. Q&A

What is MCP?

Model Context Protocol (MCP) is a protocol for structured communication with large language models (LLM).

It brings **consistency, traceability, and context awareness** into AI-driven conversations by standardizing:

- Message formats
- Session management
- Metadata embedding
- Tool calling and augmentation

Check out the release of Anthropic's MCP v1.0

Why MCP?

> “Even the most sophisticated models are constrained by their isolation from data – trapped behind information silos and legacy systems.” Anthropic, on why context integration matters

MCP gives us:

- Composable message contexts
- User/session metadata
- Better memory management
- Tool-call capabilities

Ref: HuggingFace Blog by Kseniia Shulha

Anatomy of MCP

```
{
  "mcp_version": "1.0.0",
  "session_id": "uuid-123",
  "messages": [
    {"role": "user", "content": "What is MCP?"}
  ],
  "global_metadata": {
    "user_id": "alice123",
    "locale": "en-US"
  },
  "tools": [/* tool definitions */]
}
```

Each `message` can also carry `metadata` (e.g., timestamps, source documents).

> Tip: Check out MCP docs

Message Types

MCP defines structured message roles:

- **System**: Instructions or personality definitions
- **User**: Human messages
- **Assistant**: Model responses
- **Tool Calls** (optional): Tool-calling JSON blobs

This allows predictable, auditable message flows.

Session & Context Management

MCP introduces session-level management:

- `session_id` : persistent thread context
- Sliding windows or summarization for long context
- TTL (Time to live) on messages

This helps manage memory constraints in token-limited models.

Tools and Function Calling

- LLM calls the tool
- App executes
- Inserts tool result as new assistant message

Just like OpenAI's function calling, but protocol-agnostic.

Building with MCP

Let's integrate MCP Agents into our workflows the fastest way possible!

Using GitHub Copilot!

Let's head to github blog and the mcp repo.

🙋 Q&A

Ask anything about:

- Implementing MCP
- Use cases
- Adopting MCP in production

Thank You!

- **Resources**: github.com/Alberthor47/mcp
- **Feedback**: Please fill out the survey at https://mlh.link/ghwfeedback
- **Next Steps**: Join us for Part 2!