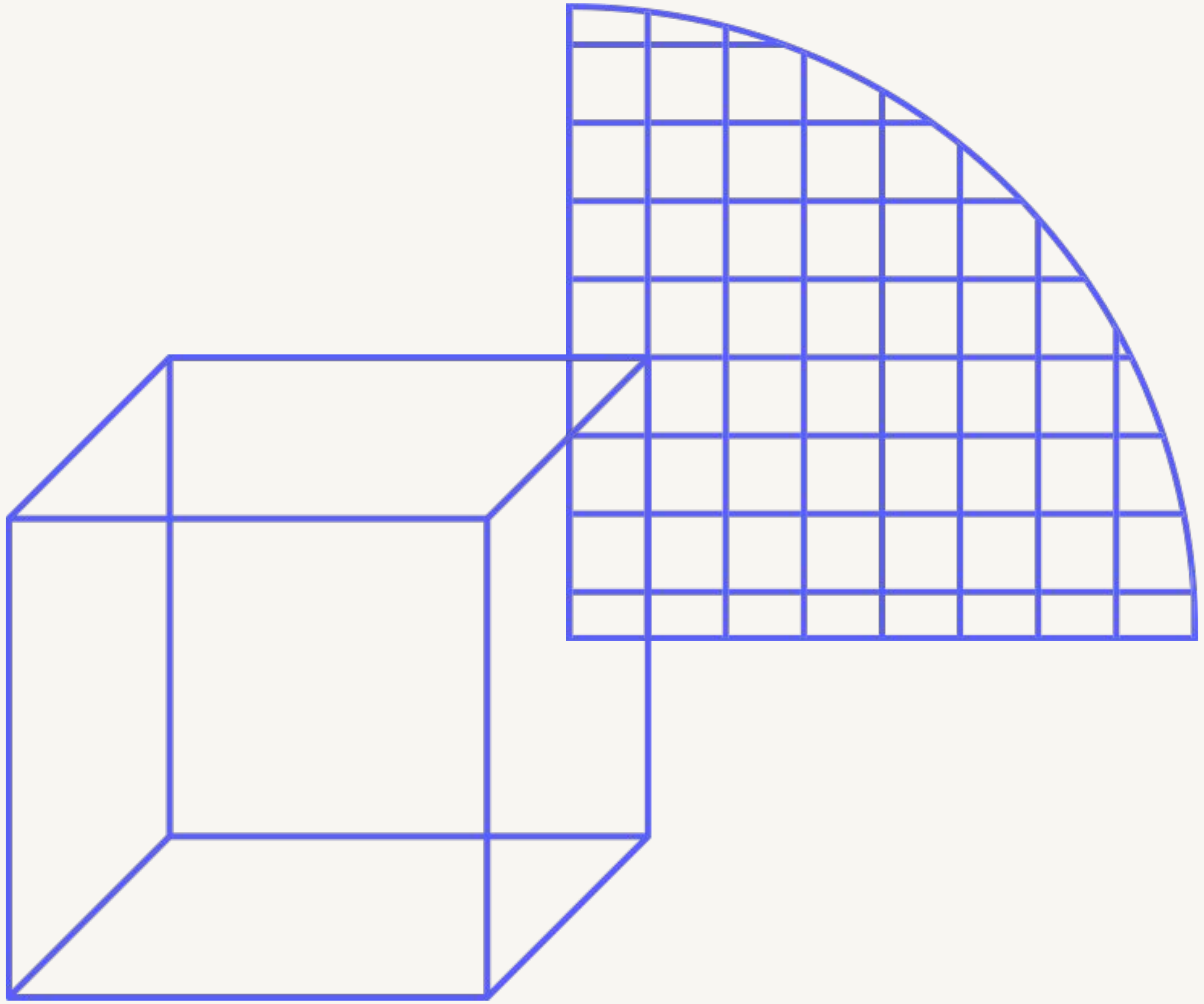
KINESIS LABS 19-APR-2025 10:00 A.M. WWW.KINESISLABS.IN

MODEL CONTEXT PROTOCOL

Standardizing AI Integration for Modern Applications



ROSHAN MISHRA

Doing Stuff with AI
@Kinesis Labs.

House Rules

While waiting for others to come in, here are some rules and reminders to keep in mind.

- ✚ Please keep your Phone in Silent Mode
- ✚ Feel free to ask your questions when they come
- ✚ Have Fun

KINESIS LABS

Today's Agenda

WHAT WE'LL LEARN:

- Quick Introduction
- LLMs, Context and History
- What is MCP and How to use it?
- How is it different from API?
- What's an MCP server and Client
- Build a small MCP server
- Q&A

Introductions

We are Kinesis Labs

I'm Roshan

I am in the Core team of Kinesis lab. I work on our agentic infrastructure. I love to build stuff (physical and digital) with AI , A lot of stuff . Early on I worked in small data ML problems to now large language Models.

Kinesis Labs

Kinesis Labs is an Applied AI Lab in Bangalore, India. Our focus is on researching and building Advanced AI tools and training the next generation of AI engineers from India.

Introductions

You are

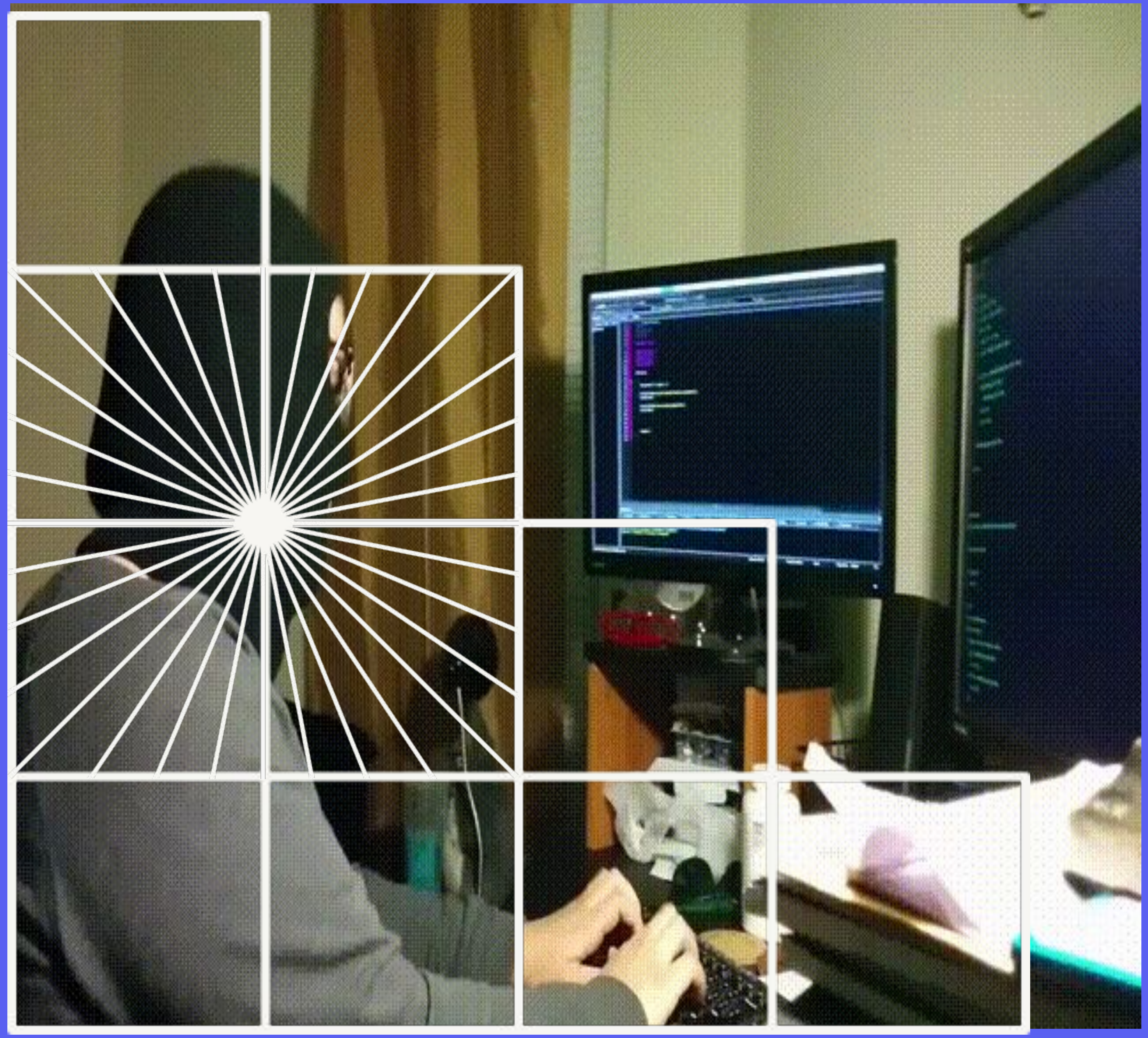
Hopefully You tell us

- Your Name and Background
- A task where you've used AI or would like AI to help you
- What do you hope to get out from the workshop

KINESIS LABS

Part I - Context

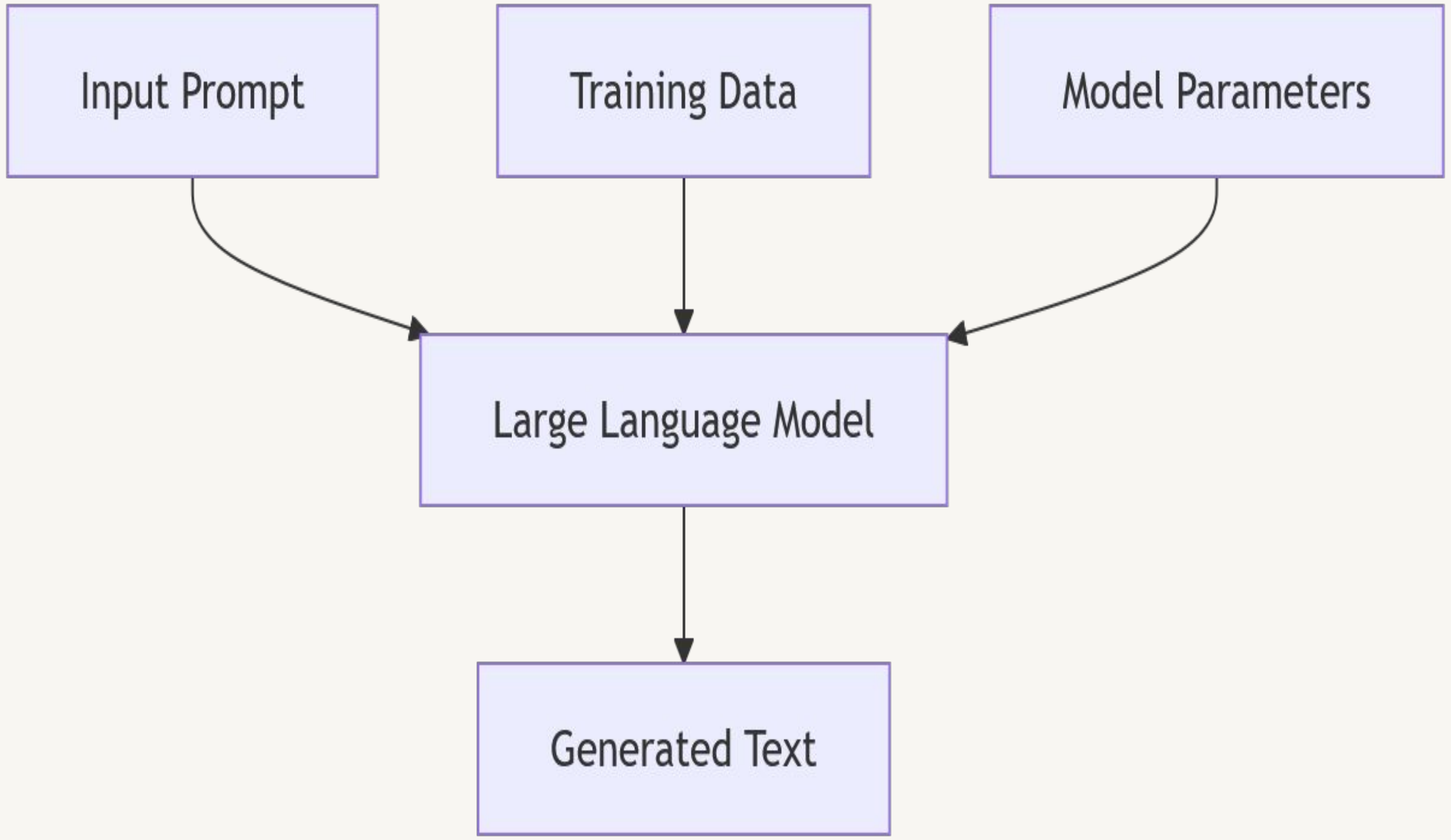
LLMs, Context and History



Understanding Large Language Models

How LLMs Work

- Trained on vast text corpora from the internet - **Training Data**
- Learn statistical patterns in language
- Generate responses by predicting what comes next - **Tokens**
- User gives a prompt
- No real-time access to external information

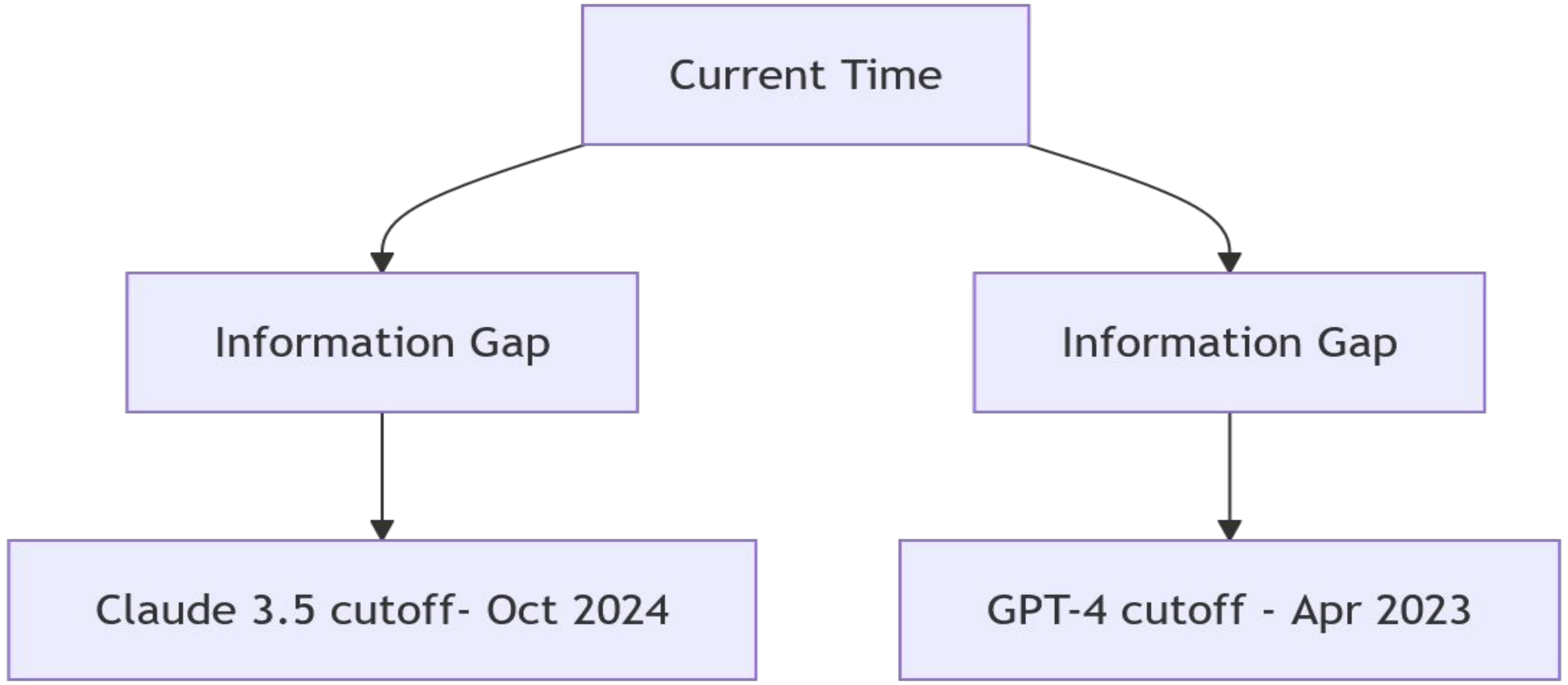


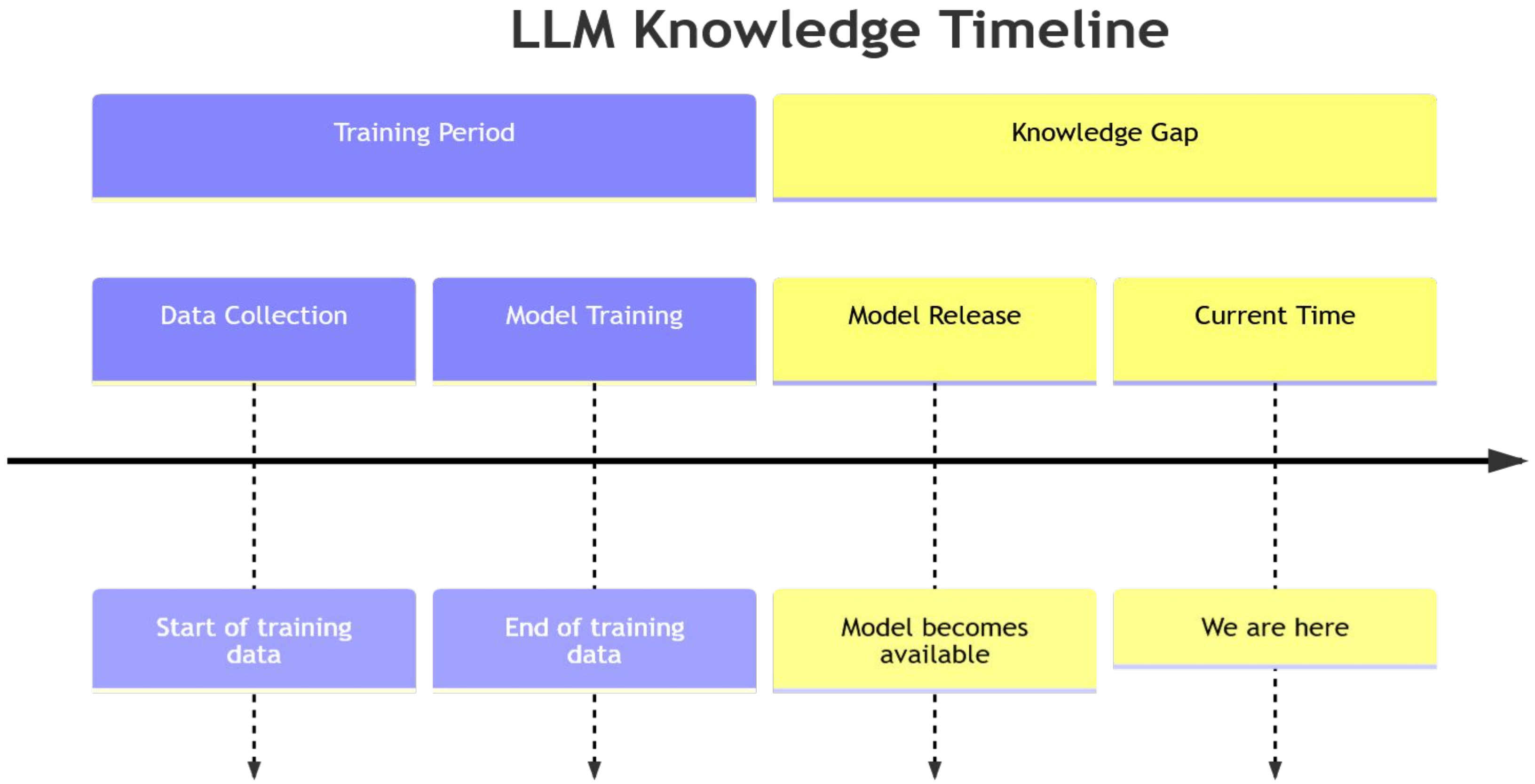
KINESIS LABS

Understanding Large Language Models

Limitations of LLMs

1. **Knowledge Cut-off** - Only trained on data available before a specific date
2. **No Real-time Information** - Can't access current data without help
3. **Hallucinations**- May generate plausible but incorrect information
4. **No External Tools** - Can't directly interact with other systems

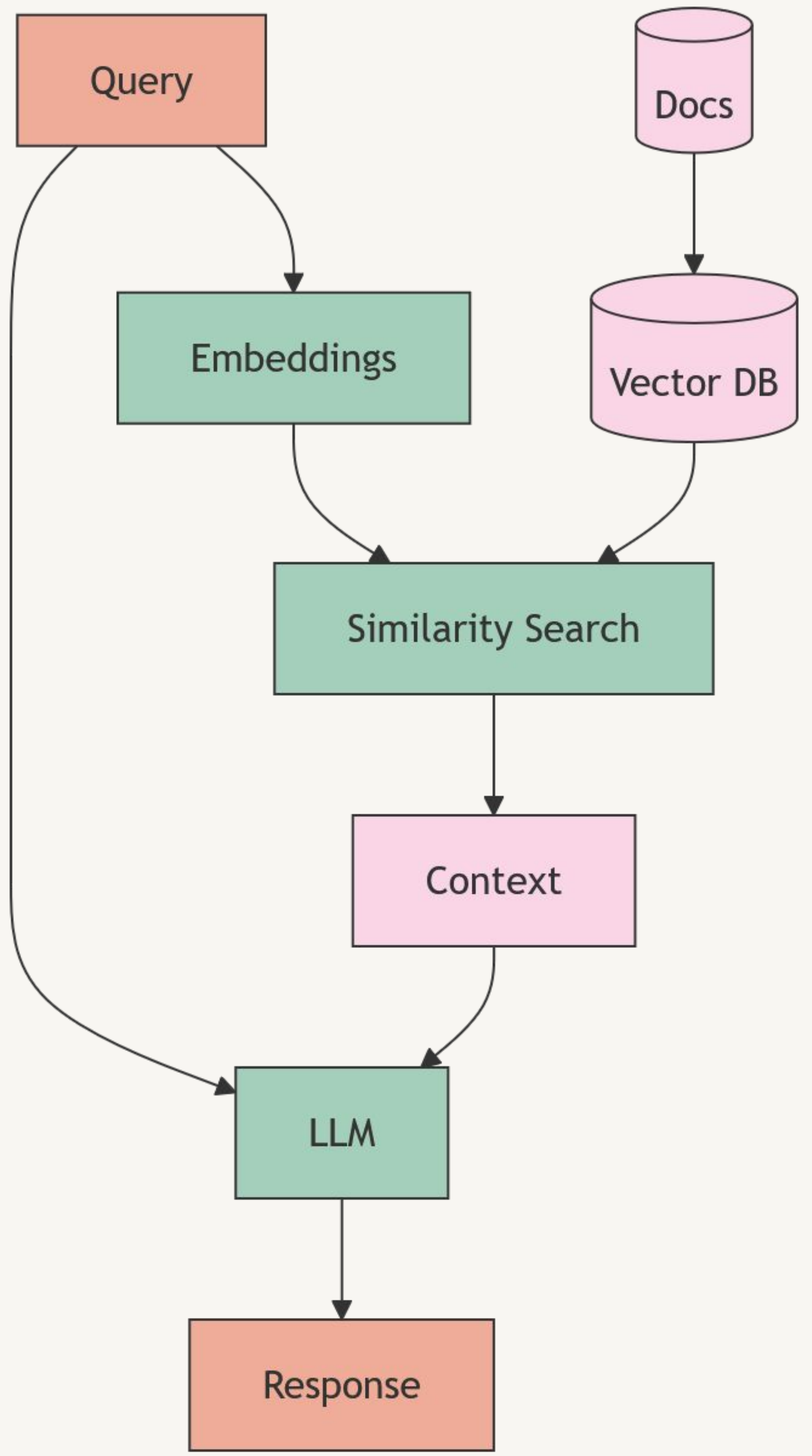




KINESIS LABS

Retrieval-Augmented Generation (RAG)

- Adds relevant external information to the LLM's context window
- Allows models to "know" things beyond their training data
- Reduces hallucinations by grounding responses in retrieved information
- Still limited to retrieve-then-generate pattern



What is Context?

It’s the build up to any story and LLMs need a lot of it to make them work long term.

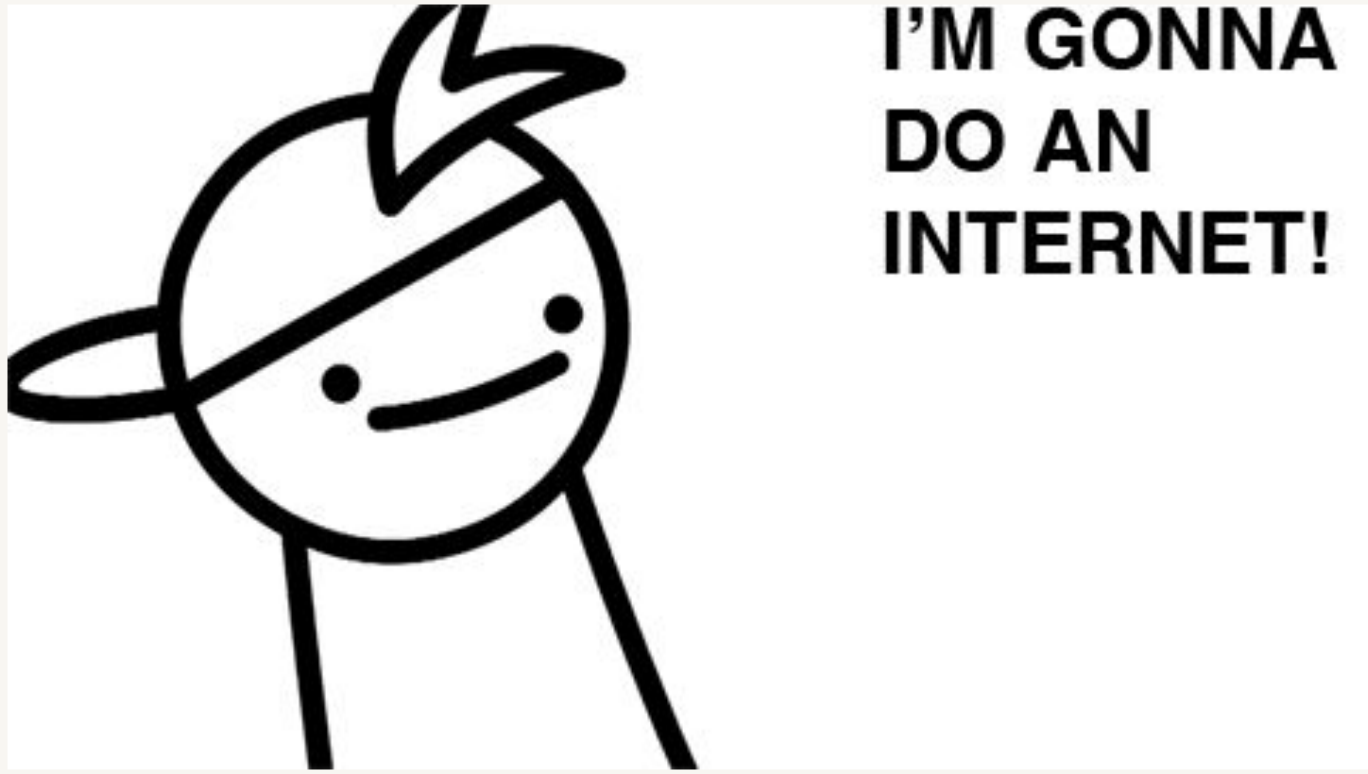
Short QnA?

Are you sleeping?

What's Model Context Protocol (MCP)?

A USB-C for LLM (what does that even mean?)

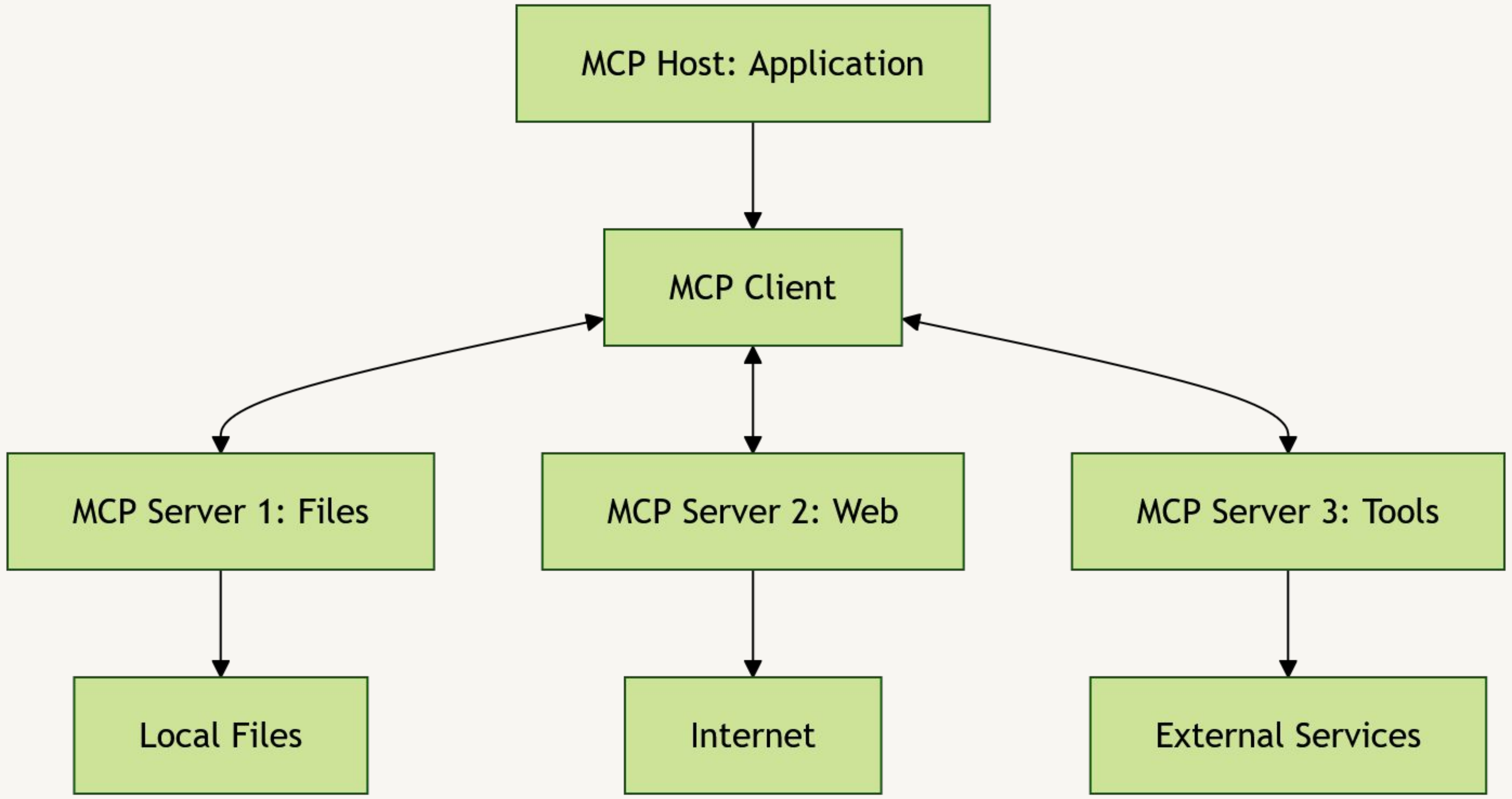
Let’s See Some MCP in Action



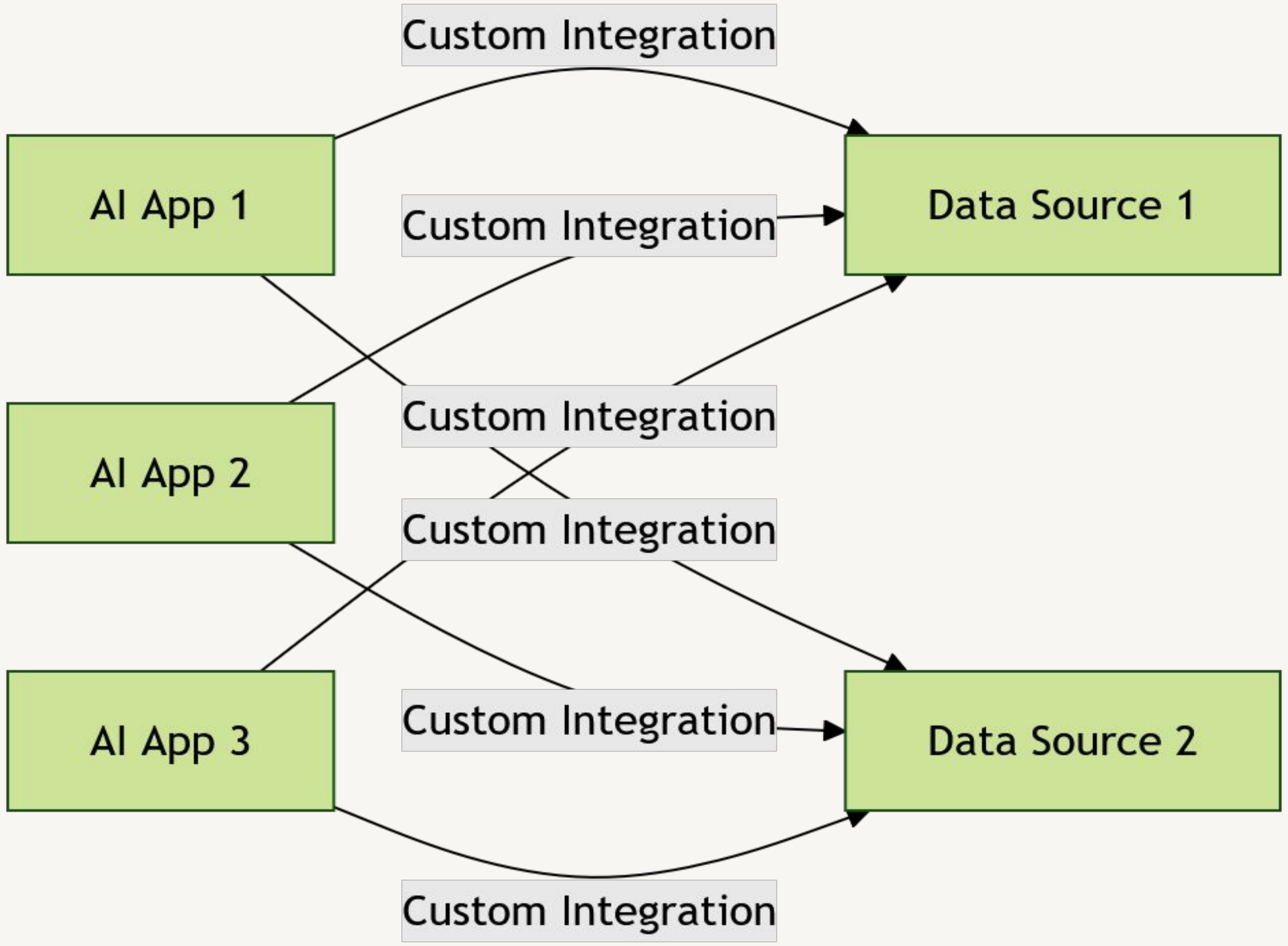
https://modelcontextprotocol.io/examples

What is MCP

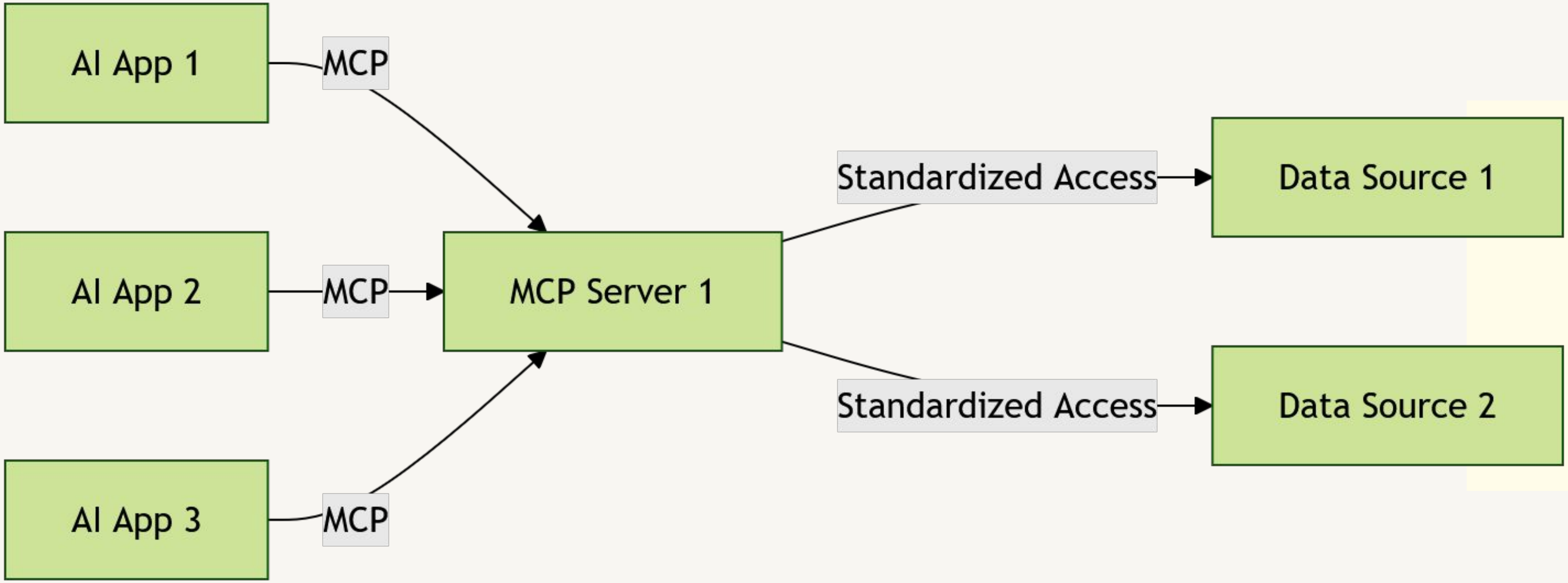
- An open standard introduced by Anthropic in late 2024
- Creates a universal way for AI assistants to connect with external data sources and tools
- Allows assistants to read files, execute code, search the web, and more
- Creates a standardized "language" for AI-tool communication

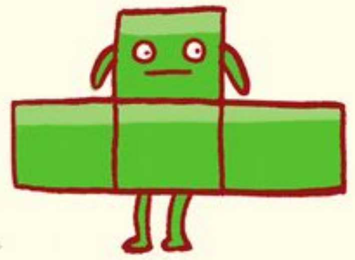


Without MCP: The Integration Problem



With MCP: Standardized Integration





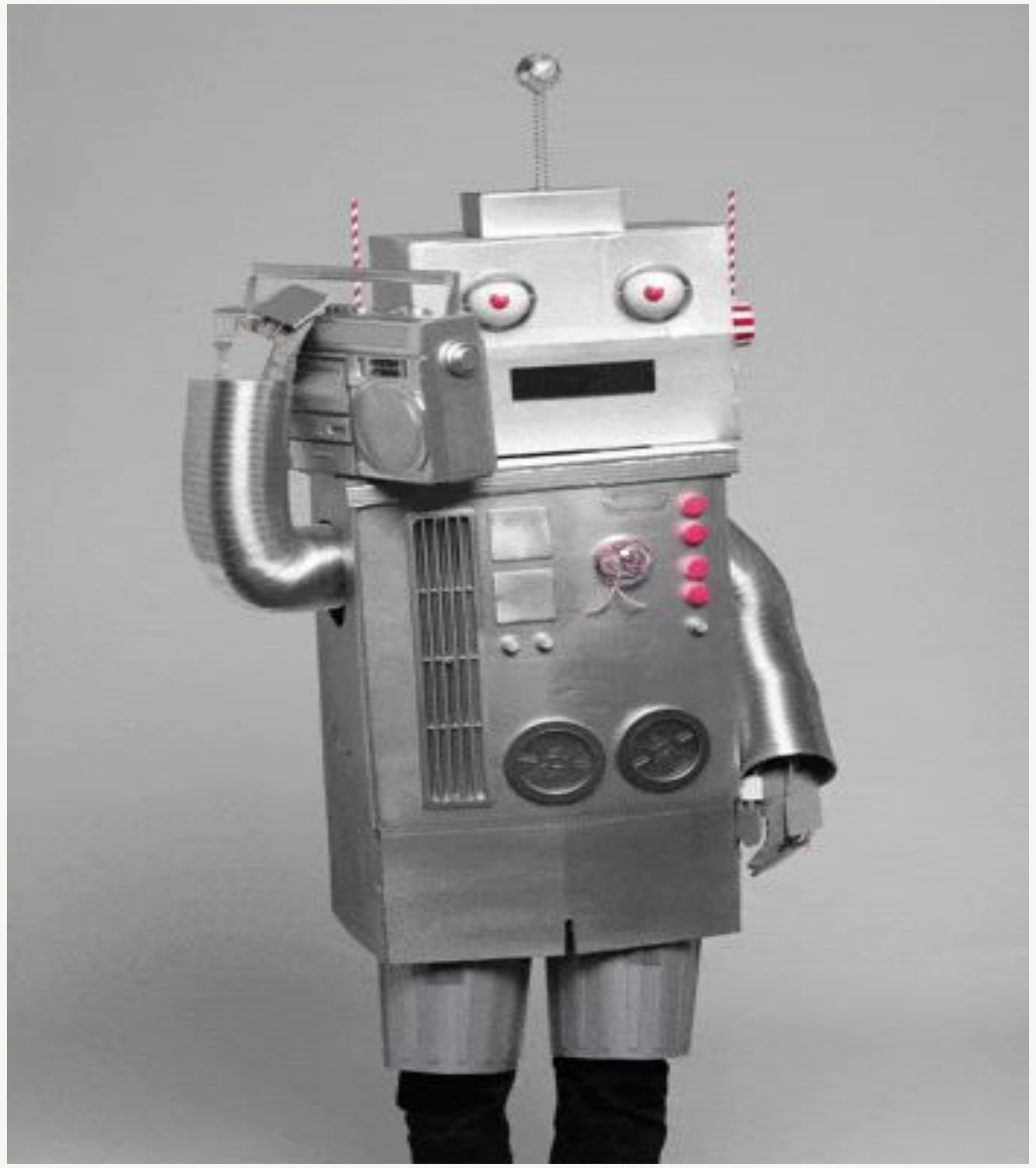
Short QnA?

Are you sleeping?

Let's See Some MCP in Action

https://modelcontextprotocol.io/examples

Benefits of MCP



Standardization: Reduces the "M×N problem" of needing custom integrations

Two-way Communication: Not just passive retrieval, but active tool use

More Relevant AI: Allows AI to access up-to-date information

User Control: Permissions model for granting access to sensitive data

Separation of Concerns: Distinct separation between data access and computation

Break : Have Some for 10 mins

Q&A

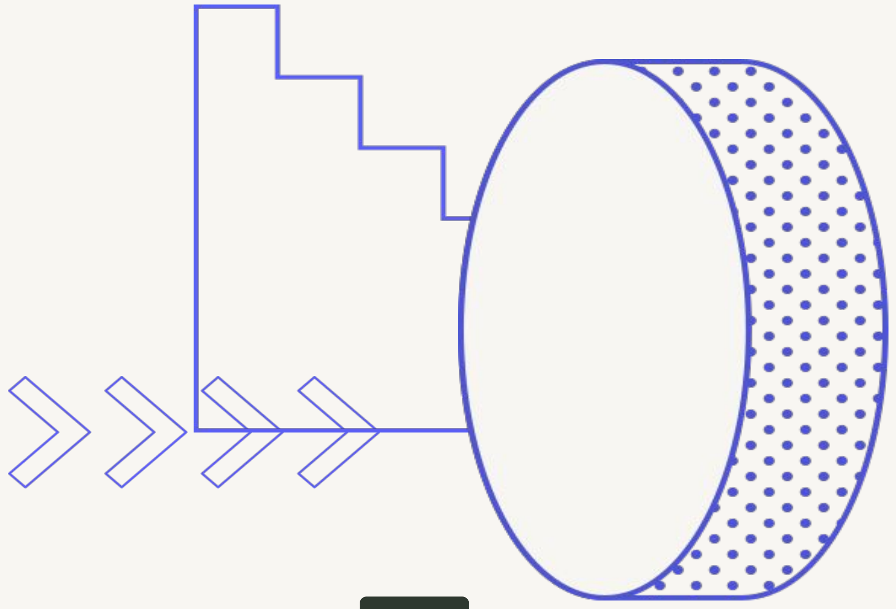
How is MCP different from API

Traditional APIs

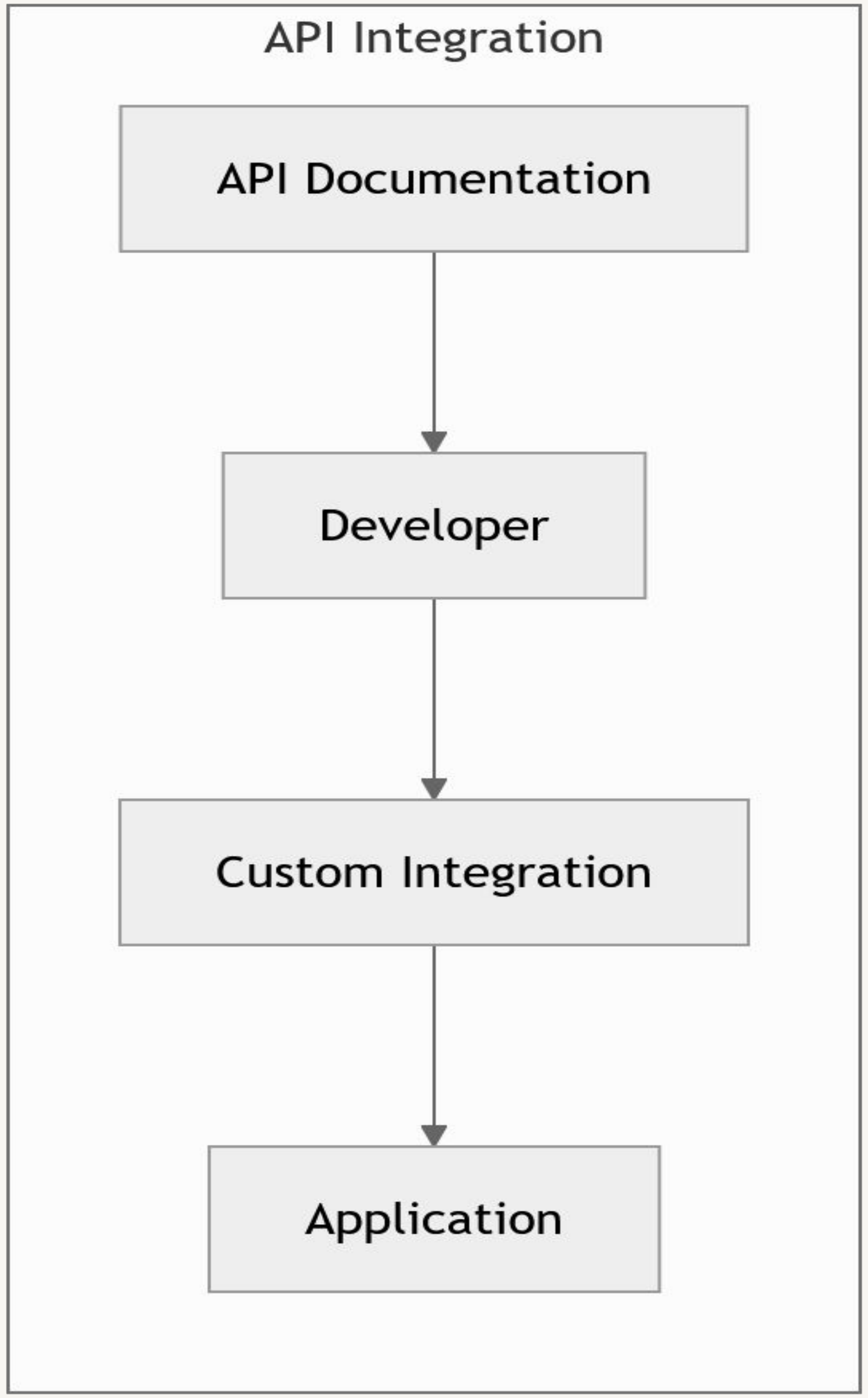
- Often complex, technical schemas|
  Static documentation
- Data structure & efficiency
- Various methods (keys, OAuth, etc.)
- Stateless, minimal context
- Technical (REST, GraphQL, etc.)

Model Context Protocol

- Human-readable descriptions
- Dynamic discovery via protocol
- Ease of use by AI models
- Standardized permissions model
- Context-aware interactions
- Natural language friendly



Traditional APIs



API Integration

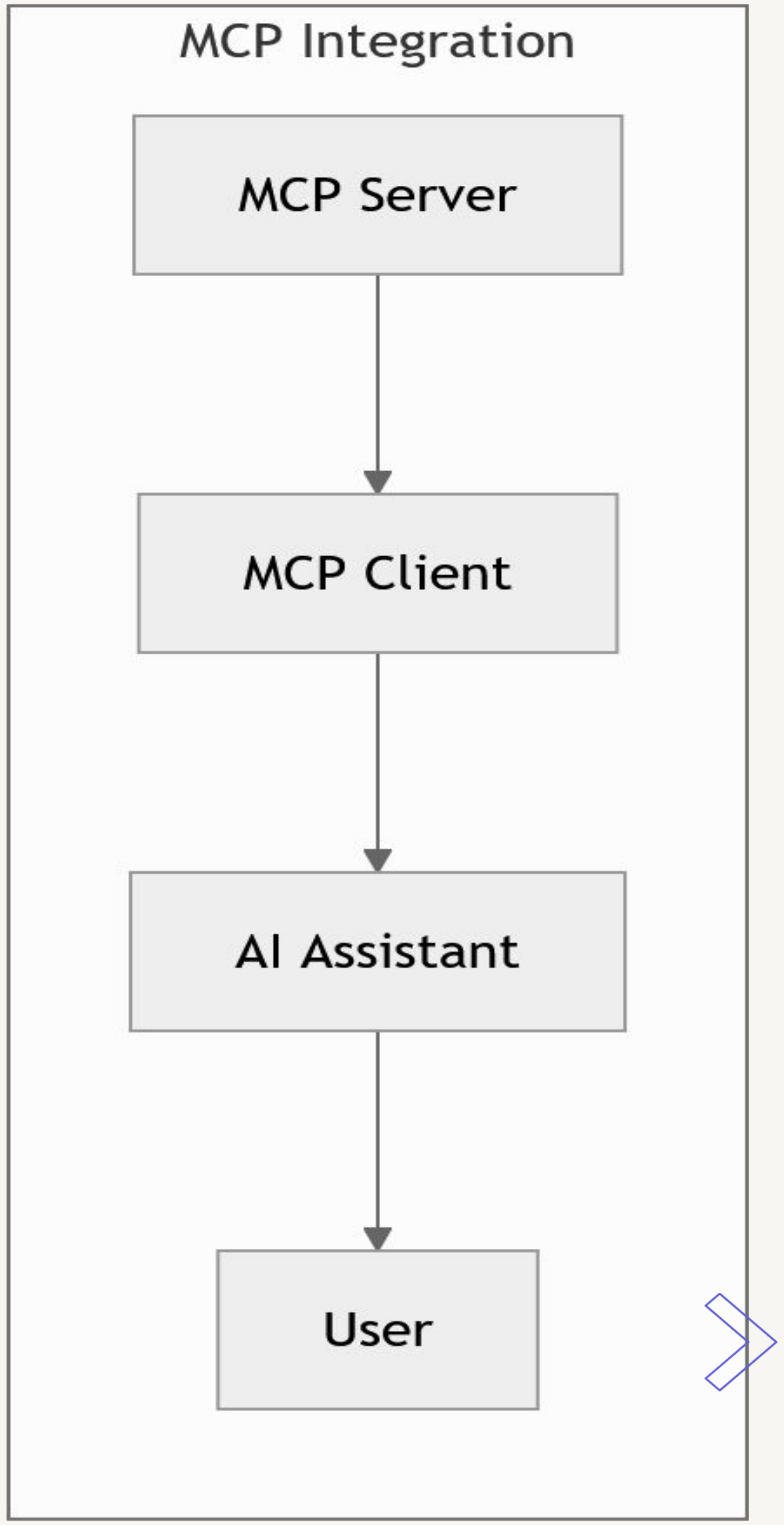
API Documentation

Developer

Custom Integration

Application

Model Context Protocol



MCP Integration

MCP Server

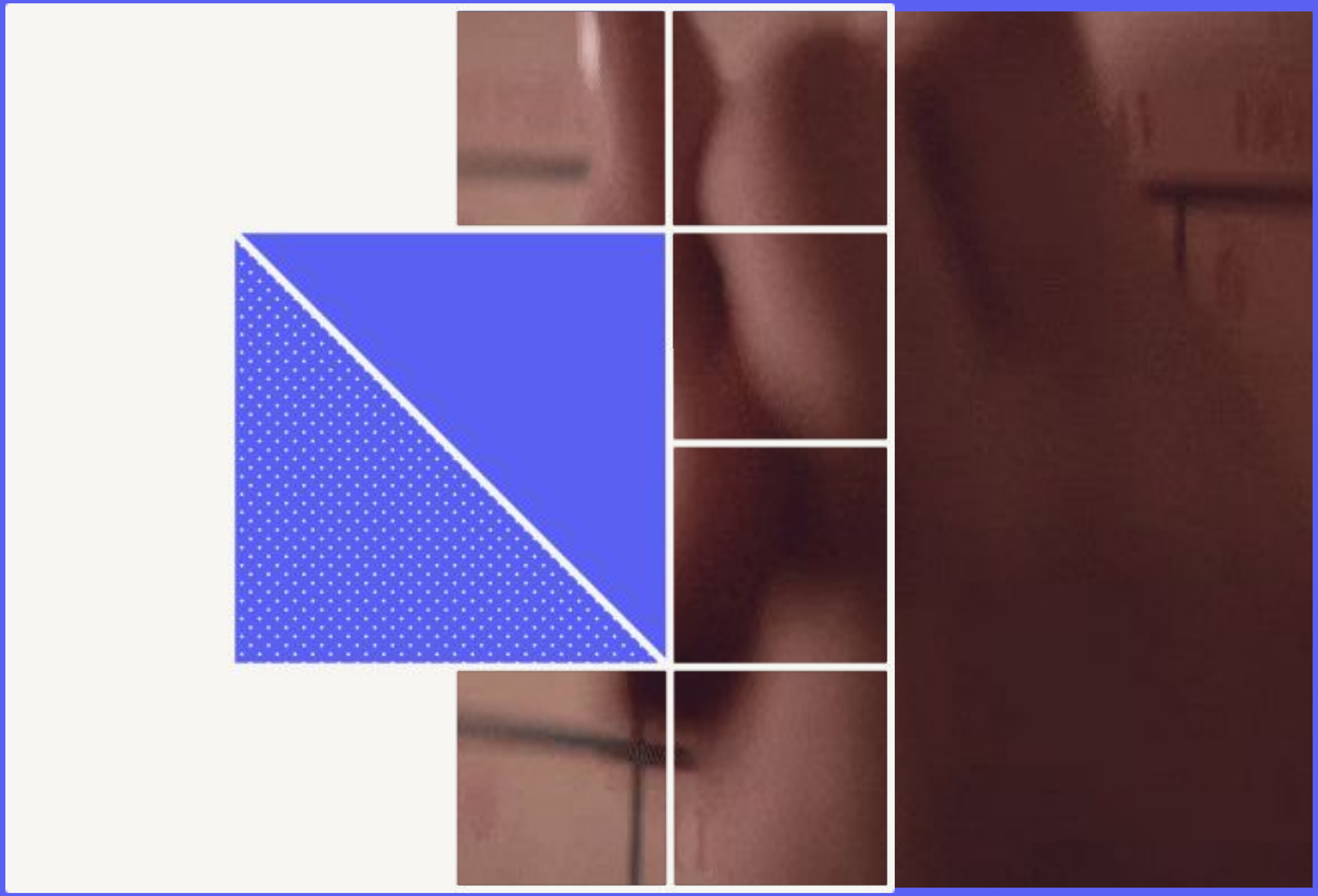
MCP Client

AI Assistant

User

MCP Internal

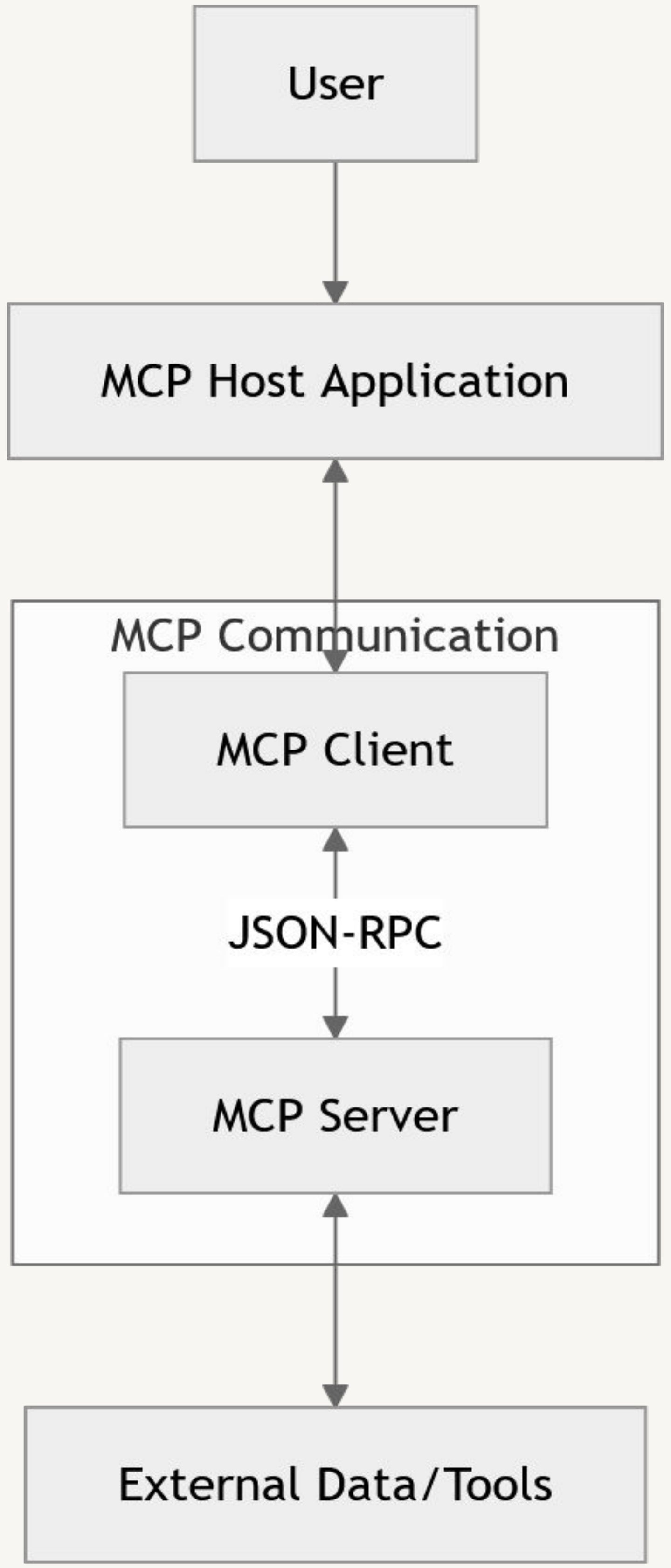
Characteristics of MCP Servers and Clients



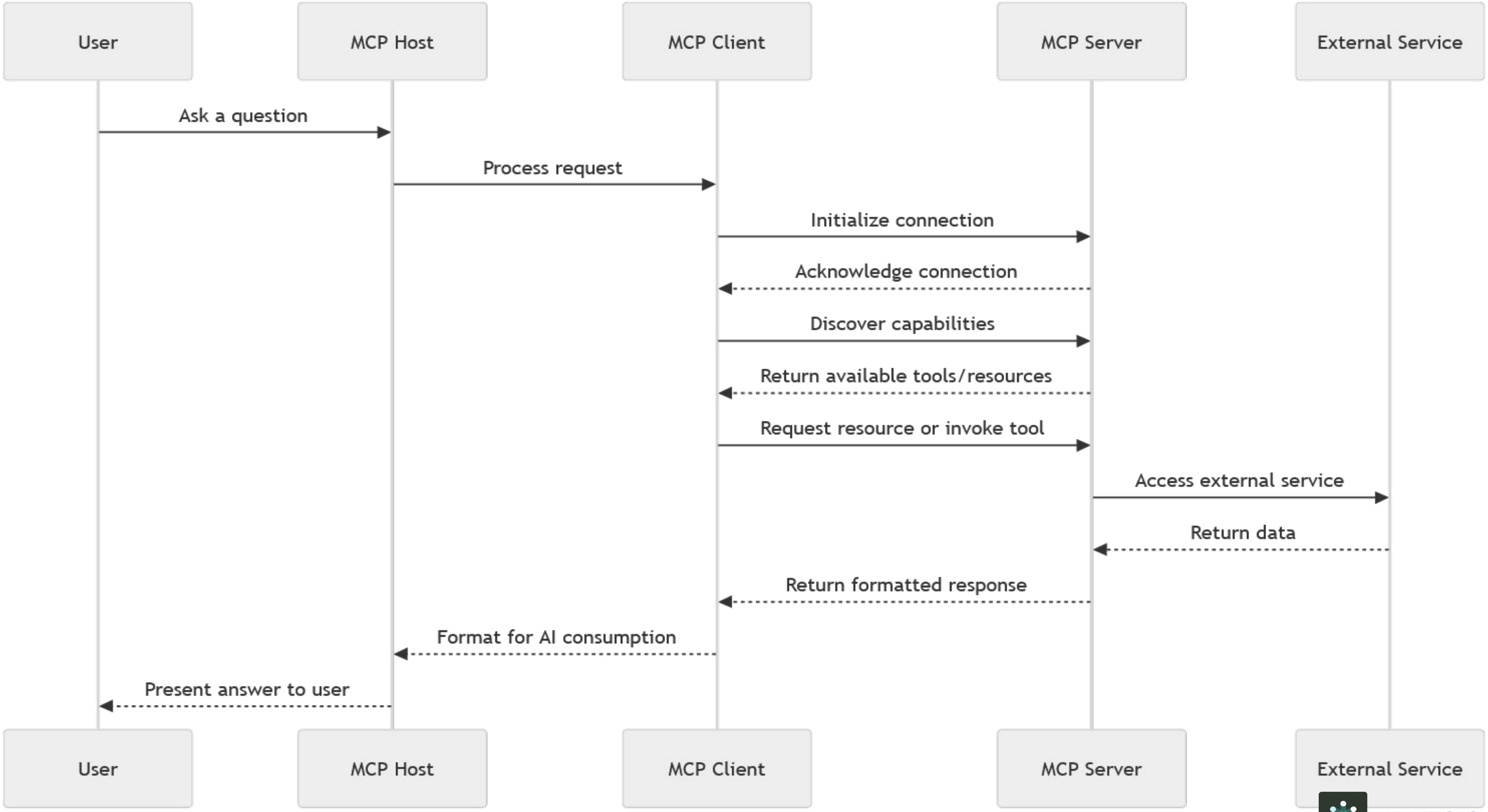
MCP Core Components

- ★ **Tools (Model-controlled)**: Functions that AI can call to perform actions
  - ○ Example: `create_file`, `send_email`, `search_web`
- ★ **Resources (Application-controlled)**: Data sources that AI can access
  - ○ Example: File contents, database records, API responses
- ★ **Prompts (User-controlled)**: Templates for guiding AI interactions
  - ○ Example: Pre-defined conversation flows for common tasks

MCP Architecture



MCP Communication Flow



MCP Characteristics

MCP Client Characteristics

- Initiates connections to MCP servers
- Manages credential and permissions
- Handles serialization and protocol details
- Provides discovery mechanisms
- Formats requests and responses for the AI model

MCP Server Characteristics

- Exposes tools and resources through standardized interface
- Handles authentication and authorization
- Executes requested operations
- Provides self-describing metadata about capabilities
- Manages connections to external systems
- Returns properly formatted responses - `JSON 2.0 - RCP`

Now Let’s Build an MCP Server

We will be Building Small Weather and AQI MCP

Push Code to Main

Short QnA?

Are you sleeping?

Thank you!

Email us your feedback

morpheus@kinesislabs.in