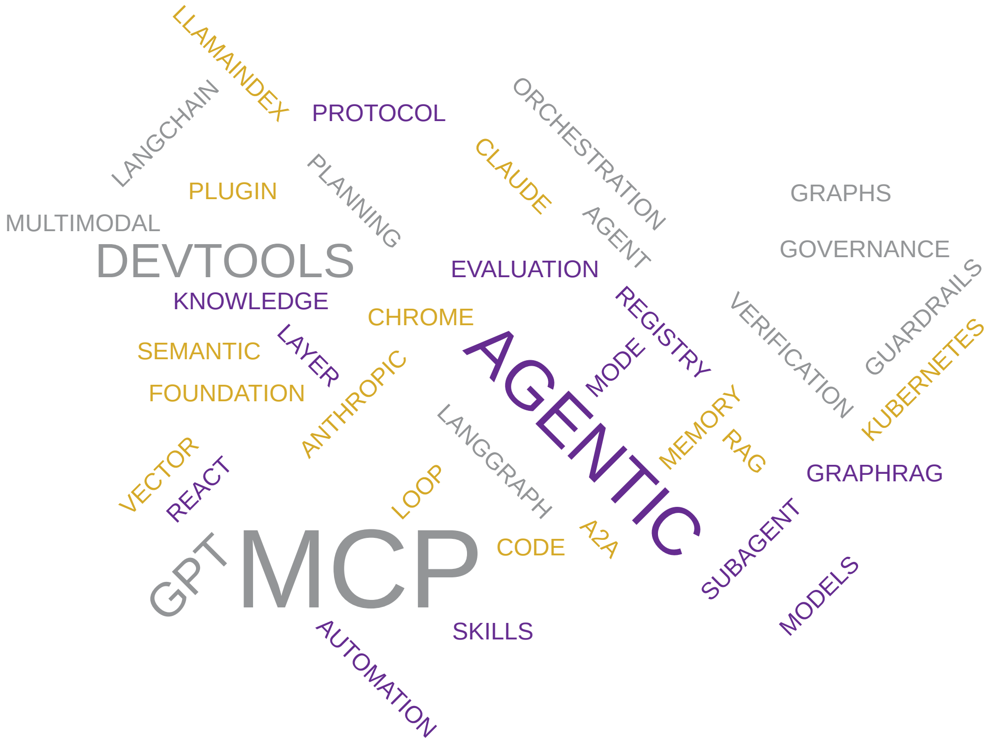

LLAMAINDEX
LANGCHAIN
PROTOCOL
ORCHESTRATION
CLAUDE
PLUGIN
PLANNING
GRAPHS
MULTIMODAL
AGENT
DEVTOOLS
GOVERNANCE
EVALUATION
KNOWLEDGE
CHROME
REGISTRY
VERIFICATION
GUARDRAILS
SEMANTIC
LAYER
AGENTIC
MODE
ANTHROPIC
FOUNDATION
KUBERNETES
MEMORY
RAG
LANGGRAPH
VECTOR
REACT
GRAPHRAG
LOOP
GPT
MCP
CODE
A2A
SUBAGENT
MODELS
SKILLS
AUTOMATION

MCP Roadmap goal: build your own MCP

Week 1: Online presentation: Ecosystem & Inspiration

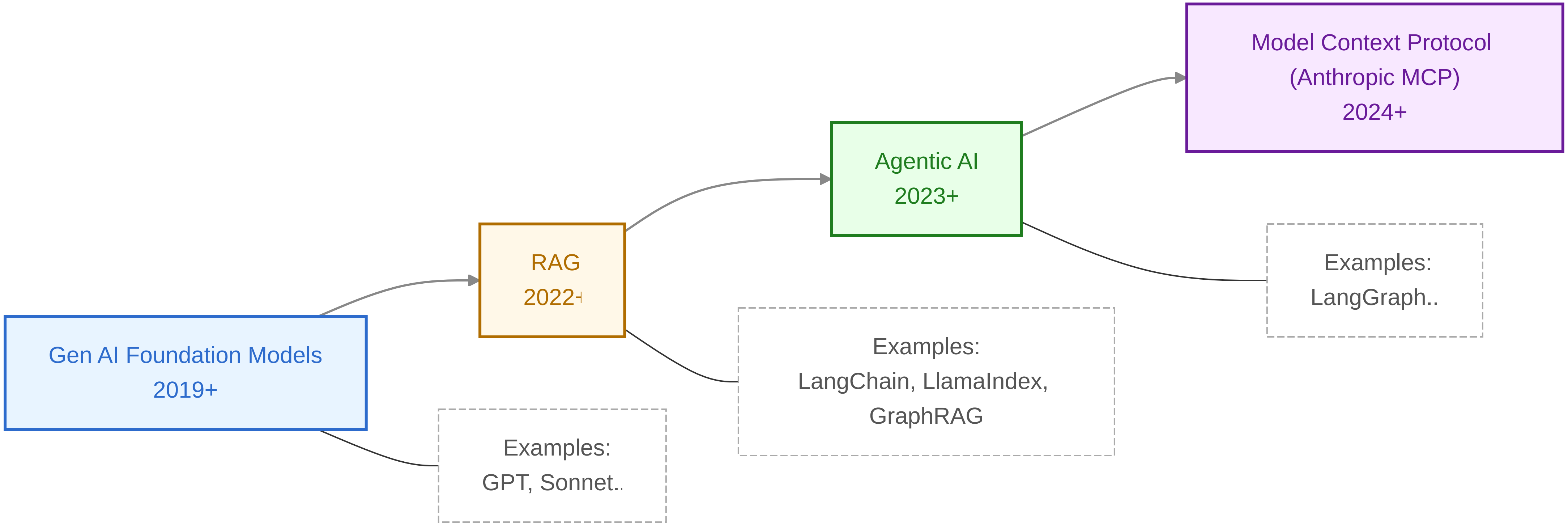
Week 2: Online presentation: Inside the Protocol

Week 3: Online presentation: Building an MCP Server

Week 4: Online Workshop: Designing Your Own Use Case

Week 5: In Office Workshop: Build & Showcase

Timeline to MCP



Gen AI Foundation Models
2019+

Examples:
GPT, Sonnet..

RAG
2022+

Examples:
LangChain, LlamaIndex,
GraphRAG

Agentic AI
2023+

Examples:
LangGraph..

Model Context Protocol
(Anthropic MCP)
2024+

🧬 Evolution: From GEN-AI to Agentic Systems

GEN-AI era: prompt → LLM → free-form text

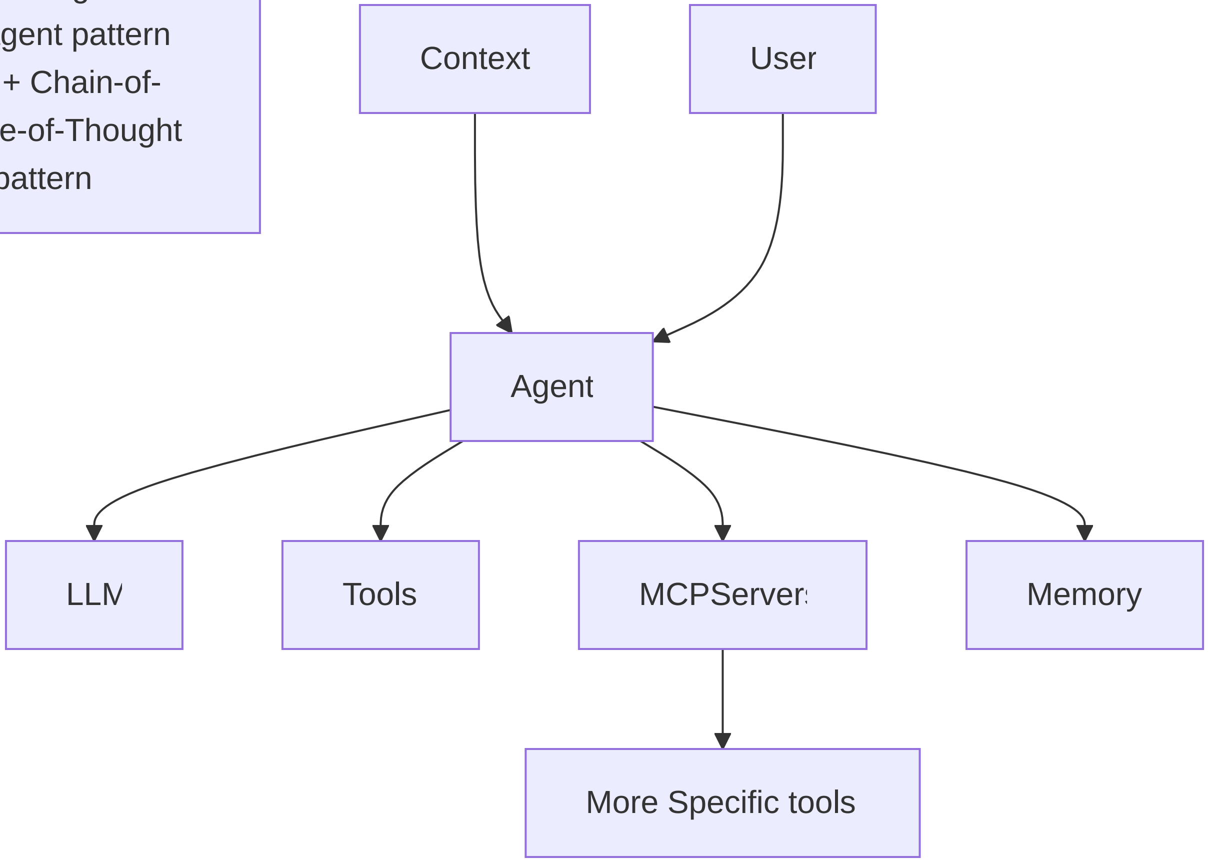
Tool / function calling: LLMs gain ability to call APIs / functions

RAG + LangChain era: vector retrieval, chains, memory

Agentic / MCP era: LLMs orchestrate tool servers, subagents, modular tool calls

🧠 The Concept of an Agent

- Planning + Tool Use + Orchestrator Agent ~workflow-agent pattern
- “Tool Use + Chain-of-Thought / Tree-of-Thought style” pattern



Model Context Protocol

AKA "USB Plug and Play for AI"

Automation

> Can I ask my agent:

- Fill my tikal timesheet ?

Automation/Scraping

Playwright

also install the playwright browser plugin

example prompts

> on the open browser tab: `https://time.infra.tikalk.dev/time.php` add entries of duration 9 for project `ABC` and task `Development` for every working day of the month

Automation/Chrome DevTools

Chrome DevTools

example prompts

> Check the performance of https://developers.chrome.com

DevOps

> Can I ask my agent:

- have all alembic migrations been applied ?

DevOps

kubernetes-mcp-server

give it your KUBECONFIG as env var

example prompts

> Retrieve the logs from the hera-web-server-* pod (last 200 lines) and summarise any ERROR or WARN messages

> have all alembic migrations been applied ?

coroot :~#

Observability

> Can I ask my agent:

- Find the root cause of the CPU jump in my kubernetes service ABC

Observability

coroot

example prompts

> using your coroot MCP server can you find out the root cause of the CPU jump in the `hera-service-pod-a738bc1397f44bbd92d194b892caeb0e` pod from 15:45 to around 16:00 ?

Cloud

> Can I ask my agent:

- List running AWS instances

Cloud

aws-api-mcp-server

Use your standard AWS credentials (env/config).

example prompts

> List all running EC2 instances in il-central-1

Risks & Limitations

Agents may choose wrong tools → robust verification needed

Registry / versioning / trust / compatibility issues

Security: sandboxing, RBAC, secrets leakage

Observability & debugging gaps in complex agent failures

Streamable HTTP is the modern, recommended transport for the Model Context Protocol (MCP), replacing the older Server-Sent Events (SSE) transport, which is now legacy.

Look out for Google's A2A Protocol. (docker vs kubernetes ?)

Takeaways & Recommendations

MCP provides standardized plumbing for tool-enabled agents

Start small (few MCP servers), then expand registry, monitoring…

Demo & Q&A

Configure your preferred agent

SourceGraph's AMP VSCode plugin

Saved prompts

Chrome devtools

Tikal Timesheet

Observability with Coroot

K8S check alembic migrations applied