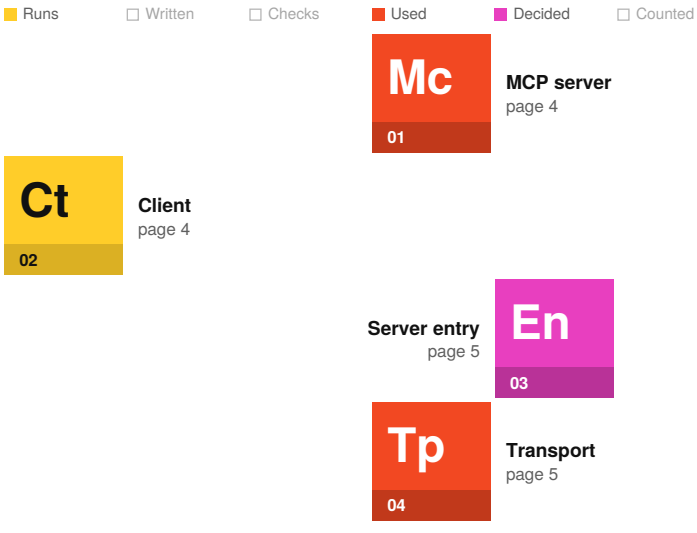
Model Context Protocol

A pocket-sized guide to MCP servers and clients, as of October 2026.



My friend has a lot of questions.

What is MCP?

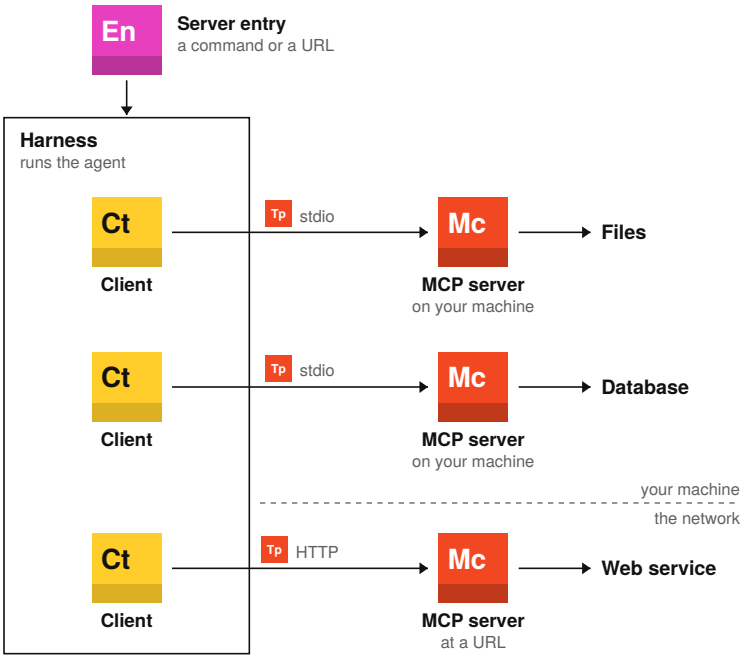
An agent can only act through tools, and the harness runs every tool call. MCP, the Model Context Protocol, is a standard way for a harness to offer the agent extra tools and data, such as your files, a database or a web service.

Someone writes a small program called an MCP server, and you add an entry for it to your harness's settings. The harness starts the server or connects to it, asks what tools it has, and passes the agent's calls to it. An Accidental Guide to: Agents, Harnesses, Skills, and Tools covers tools and tool calls.

"Server" can make you picture a service on another machine, but an MCP server is often a small program on your own machine. The harness does the asking, so in MCP the clients live in the harness.

Host	The specification's word for the harness.
MCP server	A program that offers tools and data to a harness through MCP.
Client	The part of the harness that talks to one server.
Server entry	A setting that says how to start or reach a server.
Transport	How the client and server pass messages, through stdio or HTTP.

How do the parts fit together?



The server does the reaching, with its own code and credentials, and a local server can still call a web service. The GitHub MCP server, for example, can run on your machine and call GitHub's web API, or run at GitHub's own URL.

MCP server

Mc
01

Identify by A name in the harness's MCP settings, such as github.

What **An MCP server is a program that offers tools to a harness over MCP.** Some servers also offer resources and prompts.

So what **The same server works in every harness that supports MCP.** The server holds the credentials for the system it reaches.

Field marks

Runs on	Cannot
Your machine or a URL.	**See the conversation.**

Confused with **Web service**
A web service answers requests from any program. A local MCP server often calls one, and a remote MCP server is one.

Client

Ct
02

Identify by Nothing you set up. The harness makes one for each server.

What **A client is the part of the harness that talks to one server.** The client asks the server what it offers and passes the agent's calls to it.

So what **One client per server keeps the servers apart.** A server can't see another server's calls or results.

Field marks

Runs on	Cannot
Inside the harness.	**Choose a tool.**

Confused with **Harness**
The harness is the whole program you start. A client is one part of it, so three servers mean three clients.

Server entry

En 03

Identify by An entry in `.mcp.json` for Claude Code, `~/.codex/config.toml` for Codex or `mcp.json` for VS Code, as of October 2026.

What **A server entry is a name plus the command that starts a local server or the URL of a remote one.** Commands such as `claude mcp add` write it for you.

So what **When a server's tools don't show up, check the entry first.** A wrong command, URL or key blocks the connection.

Field marks

Kept in	Cannot
A project or user file.	**Add tools by itself.**

Confused with Mc **MCP server**
The entry is a few lines of settings. The server is the program they start or point to.

Transport

Tp 04

Identify by A command or a URL in the server entry.

What **A transport is how the client and server pass messages.** With stdio, the harness starts the server on your machine. With HTTP, the server runs at a URL.

So what **When a server won't connect, check the command for stdio.** For HTTP, check the URL and sign-in.

Field marks

Runs on	Cannot
Local or remote.	**Change the tools.**

Confused with **Remote server**
HTTP usually means a remote server, but a server on your own machine can use HTTP too.

What can a server offer?

A server can offer three kinds of thing, and the difference is who picks each one.

Offer	Who picks it	Where you see it
Tools	The agent	Tool calls in the session, the same as built-in tools.
Resources	You or the harness	Data you attach, with an @ mention in Claude Code or Add Context in VS Code.
Prompts	You	Ready-made instructions you run as slash commands.

Agents mostly use tools, the only kind they pick for themselves, and as of October 2026 some harnesses support only tools.

Tip. Every tool definition takes room in the context window on every call, unless the harness loads definitions on demand, as Claude Code does by default. Add only the servers you use.

Common questions

Question	Answer
Is MCP a service?	No. MCP is a set of rules for the messages between a harness and a server.
Is MCP an AI model?	No. Your harness picks the model. MCP only carries calls, results and data.
Does an agent need MCP to use tools?	No. Built-in tools, scripts and CLIs work without it.

MCP is worth it when the same tools should work in several harnesses. Otherwise a script or CLI is often enough.

Sources

These public sources were checked in October 2026.

Model Context Protocol, Architecture overview
`modelcontextprotocol.io/docs/learn/architecture`

Model Context Protocol, Specification 2026-07-28
`modelcontextprotocol.io/specification/2026-07-28`

Anthropic, Claude Code: MCP
`code.claude.com/docs/en/mcp`

OpenAI, Codex: MCP
`learn.chatgpt.com/docs/extend/mcp`

Microsoft, VS Code: Use MCP servers
`code.visualstudio.com/docs/copilot/chat/mcp-servers`

GitHub Docs, Configure MCP servers for Copilot
`docs.github.com/en/copilot/how-tos/copilot-on-github/customize-copilot/configure-mcp-servers`



An Accidental Guide to…

Model Context Protocol

A pocket-sized guide to MCP servers and clients, as of October 2026.
Written and reviewed by a person. AI does the grunt work. Set in TeX Gyre Heros and Newsreader.
Leave a star: `accidental.info/star`

My friend has a lot of questions.