Discovery of LLM API Services in Local Networks

Initial endpoint discovery using mDNS and DNS-SD

Yihan Chao

Zhongguancun Laboratory

Co-authors: Yong Cui · Chenguang Du

draft-cui-dawn-local-llm-api-discovery-00

The problem: an API exists, but the tool cannot find it

One laptop. Two local networks.

OFFICE NETWORK

Enterprise-provided LLM API

A configured base URL works here.

HOME NETWORK

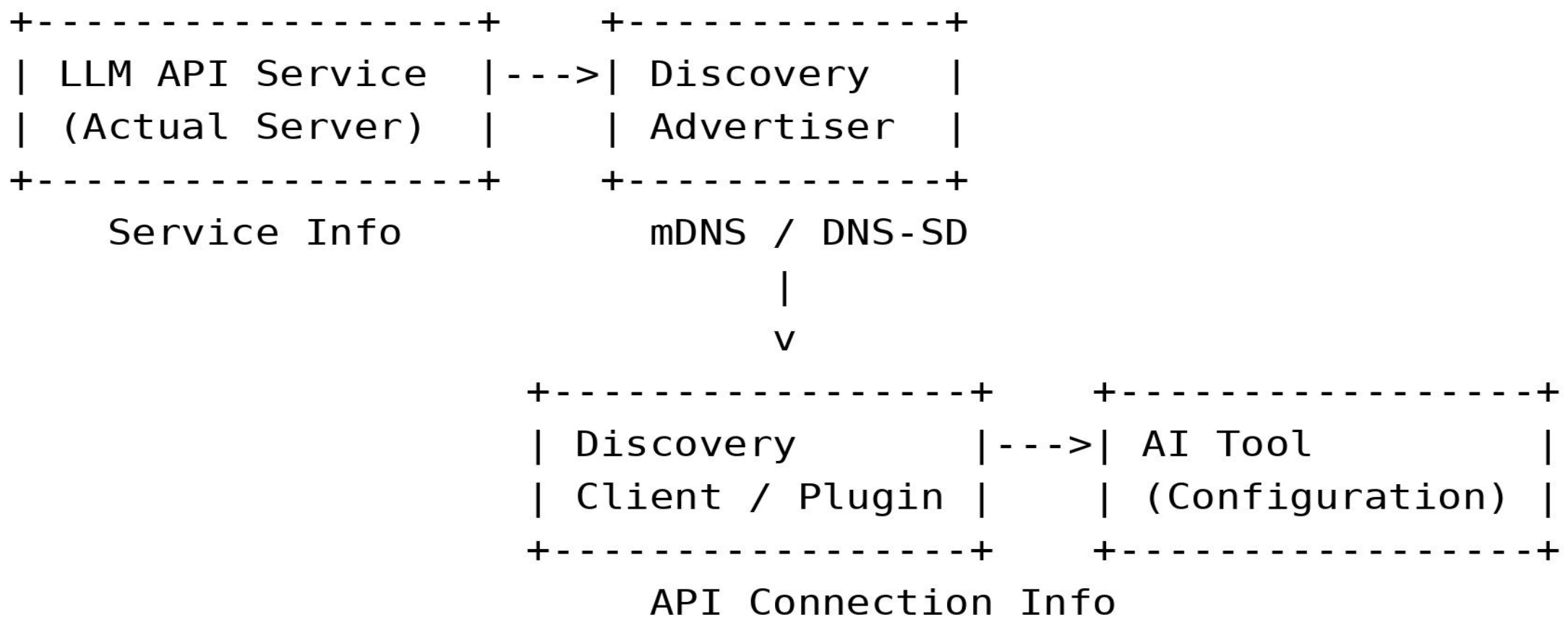
Workstation-hosted LLM API

A different base URL may be needed.

Static configuration does not follow the network — or a change of host or port.

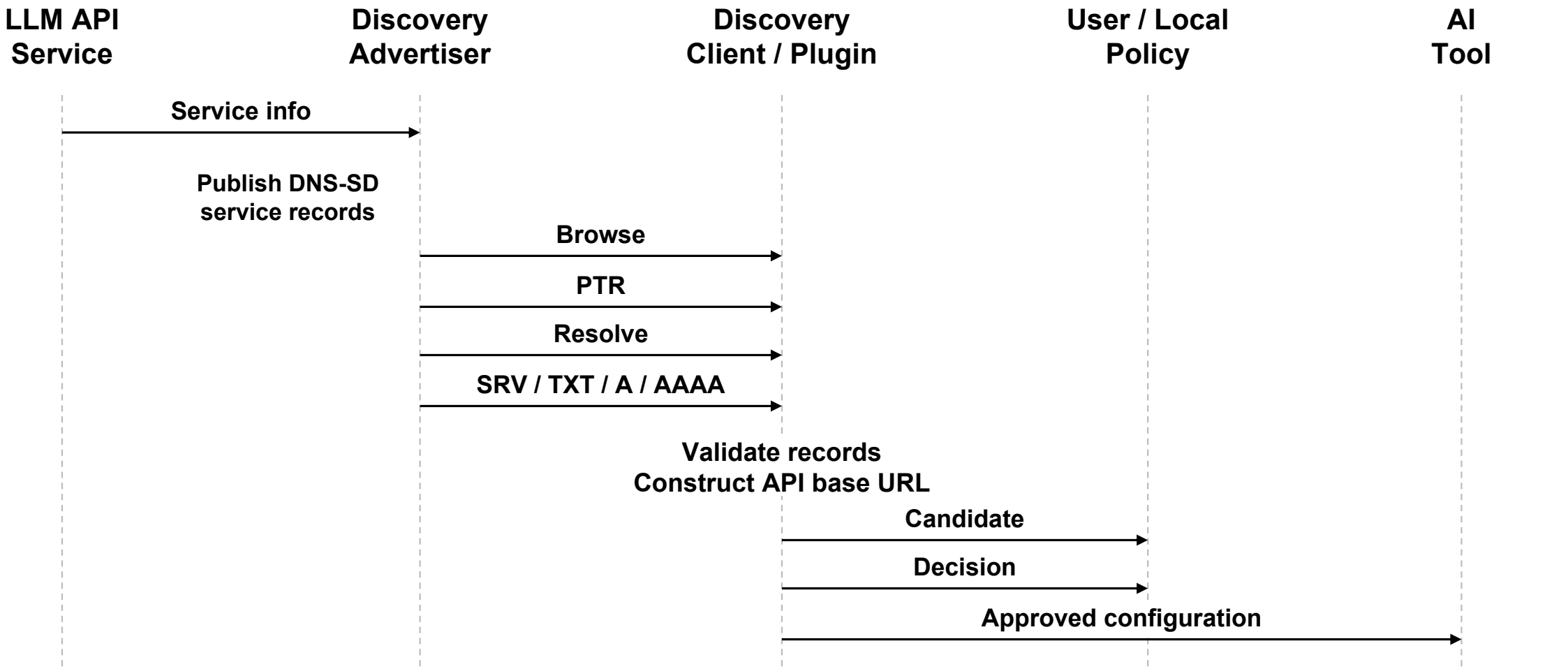
Goal: discover an API base URL and API interface profile, not credentials or model settings.

Architecture: discovery and configuration handoff



Existing mDNS / DNS-SD. No new discovery transport. No inference proxy.

Discovery sequence



What is advertised? A small DNS-SD profile

Proposed service type

_llm–api._tcp.local.

TXT parameters

txtvers	**1**
api	**openresponses**
protovers	**2026–04–24**
scheme	**https**
base	**/v1**
auth	**required**

EXAMPLE SERVICE RESOLUTION

SRV target

llm–node.local:8443

Constructed candidate base URL

https://llm–node.local:8443/v1

API profile

Open Responses 2026-04-24

POST /v1/responses

The result is a candidate — not authentication or authorization.

Discover first. Trust separately.

IN SCOPE

- Single local link
- Initial endpoint discovery
- API profile + base URL
- Candidate configuration handoff

OUT OF SCOPE

- Cross-subnet discovery
- GPU / model selection
- Credentials and API keys
- Inference messages or proxying

Discovery records are untrusted. Approve and verify the endpoint before sending sensitive data.

Feedback: service-profile interoperability and trust binding

dawn@ietf.org • datatracker.ietf.org/doc/draft-cui-dawn-local-llm-api-discovery/