

AGENT TEXT TRANSFER PROTOCOL - ATTP

Introduction

ATTP (Agent Text Transfer Protocol) is a robust networking infrastructure designed for seamless agent-to-agent communication. It encompasses essential components such as the Agent Registry, Agent Name Server (ANS), and the ATTP Protocol itself. Additionally, it ensures agent network security with features like the Agent Private Cloud (APC). The ecosystem facilitates efficient agent discovery, interaction, and communication using the ATTP protocol. Through ANS, agents can identify and connect with the most suitable counterpart for specific tasks or queries, ensuring a streamlined and secure communication process.

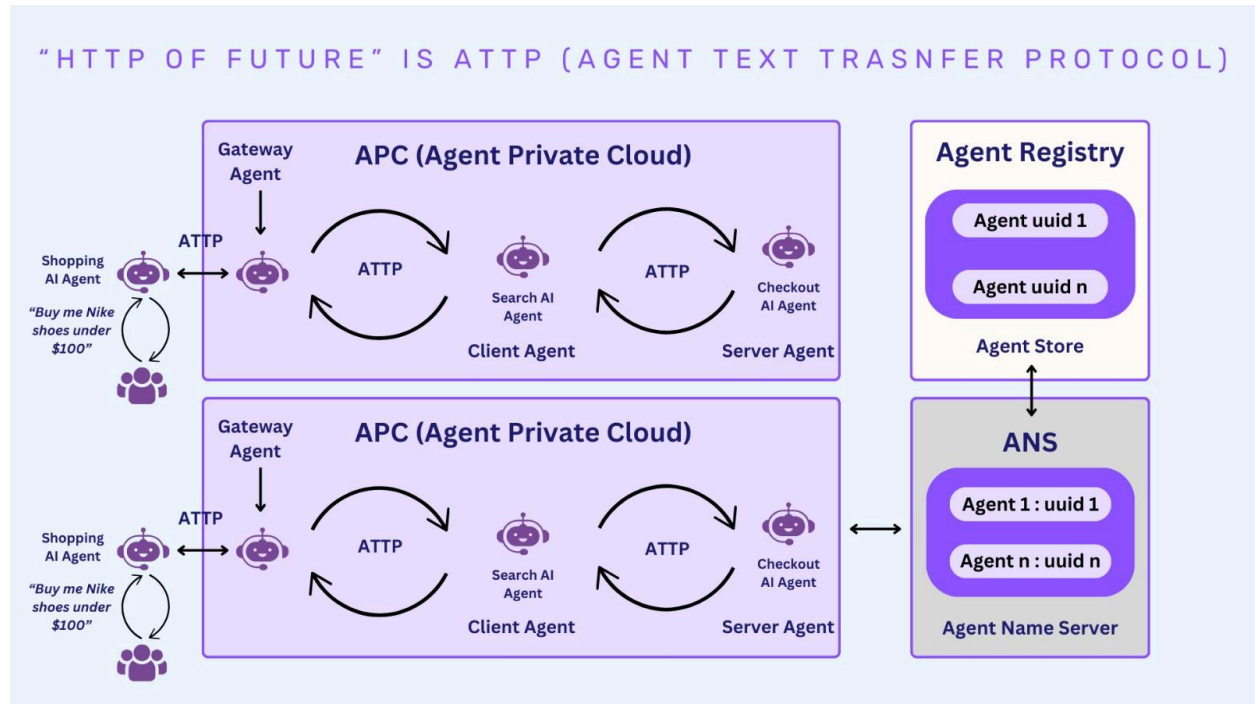
Architecture Overview

The ATTP network is composed of the following key components:

1. **Client-Agent:** This is the entry point for user queries. It extracts intent and entities from the input and initiates communication with the ANS.
2. **Agent Name Server (ANS):** Acts as a lookup service, querying the Agent Registry to resolve the intent into a specific agent UUID and its associated endpoint.
3. **Agent Registry:** A centralized repository storing agent metadata, including their UUIDs and capabilities.
4. **Server-Agent:** Processes queries received from the Client-Agent and generates appropriate responses.
5. **Agent Private Cloud (APC):** Ensures secure communication and isolated environments for sensitive agent interactions. Only agents that are part of a specific APC can communicate with each other. The APC UUID acts as an identifier for the secure network of agents.

Architecture Diagram

The architecture of ATTP is depicted in the diagram below:



Key Protocol: ATTP (Agent Text Transfer Protocol)

ATTP is the core communication protocol enabling text-based interactions between agents. It is designed to be lightweight, secure, and efficient. The protocol supports:

- Query exchange.
- Agent UUID resolution and endpoint discovery.
- Secure messaging between agents within the APC.

Protocol Details

Headers

The ATTP protocol header includes the following fields:

- Version: The version of the ATTP protocol.
- Message Type: Specifies the type of message (e.g., Request, Response, or Error).
- APC ID: The unique identifier of the Agent Private Cloud.
- Agent UUID: The unique identifier of the agent initiating and receiving the communication.
- Auth Token: A secure token for authenticating the agent within the APC.
- Timestamp: A UTC timestamp marking the time of message creation.
- Encryption Flag: Indicates whether the message is encrypted.

Body

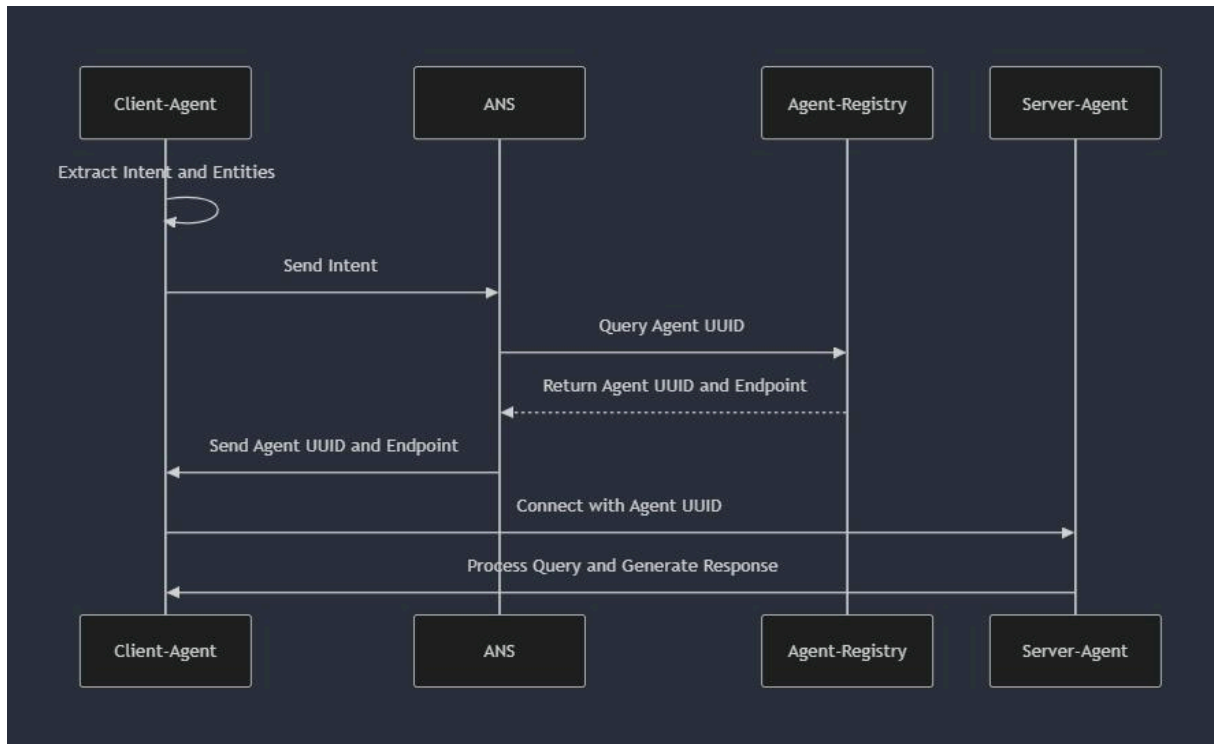
The body contains:

- Query: The user query or request for processing.

Protocol Flow

1. **Intent Extraction:** The Client-Agent receives a query, extracts the intent and entities, and prepares an ATTP request.
2. **Intent Resolution via ANS:**
 - The Client-Agent sends the intent to the ANS.
 - ANS queries the Agent Registry to find the corresponding agent UUID and endpoint.
 - ANS returns the resolved UUID and endpoint to the Client-Agent.
3. **Connection Establishment:**
 - The Client-Agent establishes a connection with the resolved Server-Agent using the UUID and endpoint.
 - The ATTP request is sent to the Server-Agent. The request includes the APC ID, Agent UUID, and Auth Token in the header for authentication and security.
4. **Query Processing:**
 - The Server-Agent processes the request, generates a response, and sends it back to the Client-Agent.
5. **Response Handling:**
 - The Client-Agent receives the response and delivers it to the user.

Sequence Diagram



Conclusion

The ATTP protocol provides a comprehensive framework for agent-to-agent communication. By leveraging ANS for efficient agent discovery and ATTP for secure messaging within the APC, it enables scalable and reliable interactions in distributed environments. This architecture is adaptable to various use cases, including automation, AI-driven workflows, and dynamic task allocation.