Network Discovery Overview

Overview of Network Discovery System

The **Network Discovery** system facilitates local network communication between different Unity applications, allowing them to discover and establish connections seamlessly on the same local network. It operates in two modes:

Server Mode

- When running as a server, the system waits for discovery broadcasts from potential clients.
- Upon receiving a broadcast, it validates the broadcast's authenticity by checking a shared authentication key hash and verifying the freshness and uniqueness of the request using timestamps and nonces.
- If the request is valid, the server responds with its network details (port and authentication token hash), enabling the client to establish a connection.

Key Components:

- **DiscoveryBroadcastData**: Sent by clients, includes hashed authentication tokens, timestamps, and unique identifiers (nonces).
- **DiscoveryResponseData**: Sent by the server as a response, containing authentication hash and network port details necessary for clients to connect securely.
- Security measures include hashing (SHA-512) for authentication and a NonceManager to prevent replay attacks.