

EntglDb Working Group
Internet-Draft
Intended status: Informational
Expires: 25 July 2026

E. Maintainers
EntglDb
21 January 2026

EntglDb Peer-to-Peer Communication and Security Protocol
draft-entglDb-p2p-protocol-00

Abstract

This document specifies the peer-to-peer communication protocol used by EntglDb, a decentralized database system. It defines the mechanisms for local node discovery via UDP, secure connection establishment over TCP using ECDH and AES-GCM, and the message framing and synchronization flow required for data consistency across nodes.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 25 July 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

| | |
|---|---|
| 1. Introduction | 2 |
| 1.1. Requirements Language | 2 |
| 2. Discovery Protocol | 2 |
| 2.1. Beacon Constants | 2 |
| 2.2. Beacon Payload | 3 |
| 3. TCP Connection and Framing | 3 |
| 3.1. Frame Structure | 3 |
| 3.2. Message Types | 3 |
| 4. Security and Handshake | 4 |
| 4.1. Phase 1: ECDH Key Exchange | 4 |
| 4.2. Phase 2: Secure Envelope | 5 |
| 5. Security Considerations | 5 |
| 6. IANA Considerations | 5 |
| 7. References | 5 |
| 7.1. Normative References | 5 |
| Author's Address | 6 |

1. Introduction

EntglDb requires a robust protocol to enable multiple nodes (peers) to discover each other on a local network, establish a secure communication channel, and synchronize data efficiently.

This specification details the wire format, discovery beacons, handshake procedures, and security requirements to ensure interoperability between different EntglDb client implementations.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Discovery Protocol

Nodes automatically discover each other using UDP broadcasts.

2.1. Beacon Constants

- * *Port:* 25000
- * *Interval:* 5000 ms
- * *Transport:* UDP Broadcast/Multicast

2.2. Beacon Payload

The payload MUST be a UTF-8 encoded JSON string adhering to the following structure:

```
{
  "node_id": "UUID-STRING",
  "tcp_port": 25000
}
```

Receiving nodes MUST ignore beacons originating from their own node_id.

3. TCP Connection and Framing

Upon discovery, a node initiates a TCP connection to the advertised IP and tcp_port.

3.1. Frame Structure

All messages sent over the TCP stream MUST adhere to the following length-prefixed format. All integers are Little Endian.

```
+-----+-----+-----+-----+
| Length (4 bytes) | Type (1 byte) | Compress (1 byte) | Payload (N bytes) |
+-----+-----+-----+-----+
```

* *Length:* 32-bit signed integer representing the size of the *Payload* only. It does NOT include the header size (6 bytes).

* *Type:* 1-byte enum identifying the message type.

* *Compression:* 1-byte flag. 0x00 = None, 0x01 = Brotli.

* *Payload:* The serialized Protocol Buffer message.

3.2. Message Types

The Type byte corresponds to the following values:

| ID | Name | Description |
|----|----------------|-------------------------------|
| 1 | HandshakeReq | Connection connection request |
| 2 | HandshakeRes | Connection response |
| 3 | GetClockReq | Request current HLC |
| 4 | ClockRes | HLC response |
| 5 | PullChangesReq | Request Oplog diff |
| 6 | ChangeSetRes | Send batch of changes |
| 7 | PushChangesReq | Proactive changes push |
| 8 | AckRes | Receipt confirmation |
| 9 | SecureEnv | Encrypted envelope |

Table 1

4. Security and Handshake

Security is mandatory. The protocol enforces an encrypted channel using ECDH for key exchange and AES-GCM for confidentiality and integrity.

4.1. Phase 1: ECDH Key Exchange

Before any Protobuf messages are exchanged, a raw key exchange occurs:

1. **Initiator** sends: 4-byte Length + Public Key (NIST P-256 SubjectPublicKeyInfo).
2. **Responder** sends: 4-byte Length + Public Key (NIST P-256 SubjectPublicKeyInfo).

Both parties compute the **Shared Secret**. Session keys are derived using a simplified HKDF-like scheme:

- * Key1 = SHA256(Secret || 0x00)
- * Key2 = SHA256(Secret || 0x01)

The Initiator uses Key1 for encryption and Key2 for decryption. The Responder uses Key2 for encryption and Key1 for decryption.

4.2. Phase 2: Secure Envelope

After key exchange, ALL subsequent frames MUST have Type = 9 (SecureEnv).

The payload of a SecureEnv message is a Protobuf SecureEnvelope:

```
message SecureEnvelope {  
  bytes ciphertext = 1;  
  bytes nonce = 2; // 12 bytes  
  bytes auth_tag = 3; // 16 bytes  
}
```

The **plaintext** inside the encrypted ciphertext contains the inner wire format:

```
[Type (1 byte)] [Compression (1 byte)] [Inner Payload]
```

5. Security Considerations

This protocol relies on the strength of NIST P-256 and AES-256-GCM. Implementers MUST ensure secure random number generation for ephemeral keys and nonces.

**Authentication:* While the current handshake encrypts traffic, robust node authentication relies on the *auth_token* field in the HandshakeReq. Implementations SHOULD verify this token against a trusted authority or ACL.

**Man-in-the-Middle (MitM):* The current ECDH exchange is anonymous. To prevent MitM attacks, future versions MAY include signing of the ephemeral public keys using a long-term identity key.

6. IANA Considerations

This document registers the following UDP/TCP port for EntglDb Discovery and Synchronization:

* **Port:* 25000

* **Use:* EntglDb Beacon (UDP) and Sync Protocol (TCP)

7. References

7.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

Author's Address

EntglDb Maintainers
EntglDb
Italy
Email: info@entglDb.com