Mathematical Mesh 3.0 Part XI: Mesh Presence Service

Mesh Presence Service

<series>draft-hallambaker-mesh-presence

<status>informational

<stream>independent

<ipr>trust200902

<author>Phillip Hallam-Baker

<surname>Hallam-Baker

<initials>P. M.

<firstname>Phillip

<email>phill@hallambaker.com

<organization>ThresholdSecrets.com

<keyword>Threshold Cryptography

<keyword>Elliptic Curve

<keyword>Threshold Encryption

<keyword>Threshold Key Generation

<keyword>Ceremony

Discussion of this draft should take place on the MathMesh mailing list (mathmesh@ietf.org), which is archived at <https://mailarchive.ietf.org/arch/browse/mathmesh/>.

# Introduction

Mesh Presence Protocol (MPP) is a UDP publish/subscriber protocol. Devices subscribed to an event notification service associated with an account receive UDP notification of events posted to that channel. This service may be used to provide subscribing devices with immediate of an event without the need for polling.

Uses of the presence service include notifying a device that an inbound synchronous communication session has been requested, receipt of an asynchronous message, updates to a Mesh catalog, etc.

MPP provides NAT traversal capabilities similar to those provided by STUN <info="rfc8489">. Combining these capabilities with a presence service avoids the need for a separate service.

All MPP packets are encapsulated as RUD datagrams. Messages from the client to the service are limited to a single packet. Messages from the service to the client may contain between 1 and 16 packets.

# Definitions

This section presents the related specifications and standards....

## Related Specifications

The Mesh Callsign registry is a component part of the Mathematical Mesh <norm="draft-hallambaker-mesh-architecture"/> and makes use of the data formats and service formats described therein. In particular:

Uniform Data Fingerprint <norm="draft-hallambaker-mesh-udf"/>.

Describes the UDF format used to represent cryptographic nonces, keys and content digests in the Mesh and the use of Encrypted Authenticated Resource Locators (EARLs) and Strong Internet Names (SINs) that build on the UDF platform.

Data at Rest Encryption <norm="draft-hallambaker-mesh-dare"/>.

Describes the cryptographic message and append-only sequence formats used in Mesh applications and the Mesh Service protocol.

JSON-BCD Encoding <norm="draft-hallambaker-jsonbcd"/>.

Describes extensions to the JSON serialization format to allow direct encoding of binary data (JSON-B), compressed encoding (JSON-C) and extended binary data encoding (JSON-D). Each of these encodings is a superset of the previous one so that JSON-B is a superset of JSON, JSON-C is a superset of JSON-B and JSON-D is a superset of JSON-C.

## Defined Terms

This document makes use of the terms defined in <norm="draft-hallambaker-mesh-architecture"/>.

## Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 <norm="RFC2119"/>.

## Implementation Status

The implementation status of the reference code base is described in the companion document <info="draft-hallambaker-mesh-developer"/>.

<include=..\Examples\Colophon.md>

# Message Format

# Protocol

## Client Initiated

Client initiated messages MAY be sent via either Web Service transport or UDP transport.

### Subscribe

The

#### Request

#### Responses

### Unsubscribe

#### Request

#### Response

### Status

The status interaction requests that the service resend the last publication message sent.

#### Request

The Status Response message

#### Response

### DNS Proxy

#### Request

#### Response

## Service Initiated

Service initiated messages MUST be sent via UDP transport

### Publish

The publish message is

#### Status

Serial

Serial number of the status response.

IP Endpoint

The IP Endpoint from which the last UDP communication from the client was received.

DateTime

The current date and time in ticks and leap seconds.

Store Status

A list of status values for stores that have been updated.

#### Acknowledgement

The acknowledgement message acknowledges receipt of a Status message.

# UDP Transport Binding

## Service to Client Message

## Client to Service Message

# IANA Considerations

This document requires no IANA actions.

# Acknowledgements